S. HRG. 109–195

Senate Hearings

Before the Committee on Appropriations

Department of Homeland Security

Fiscal Year 2006

109*th* CONGRESS, FIRST SESSION

H.R. 2360

DEPARTMENT OF HOMELAND SECURITY
NONDEPARTMENTAL WITNESSES

Department of Homeland Security, 2006 (H.R. 2360)

S. HRG. 109–195

DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR FISCAL YEAR 2006

HEARINGS

BEFORE A

SUBCOMMITTEE OF THE

COMMITTEE ON APPROPRIATIONS

UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

ON

H.R. 2360

AN ACT MAKING APPROPRIATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY FOR THE FISCAL YEAR ENDING SEPTEMBER 30, 2006, AND FOR OTHER PURPOSES

Department of Homeland Security
Nondepartmental witnesses

Printed for the use of the Committee on Appropriations

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

99–863 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON APPROPRIATIONS

THAD COCHRAN, Mississippi, *Chairman*

TED STEVENS, Alaska
ARLEN SPECTER, Pennsylvania
PETE V. DOMENICI, New Mexico
CHRISTOPHER S. BOND, Missouri
MITCH McCONNELL, Kentucky
CONRAD BURNS, Montana
RICHARD C. SHELBY, Alabama
JUDD GREGG, New Hampshire
ROBERT F. BENNETT, Utah
LARRY CRAIG, Idaho
KAY BAILEY HUTCHISON, Texas
MIKE DEWINE, Ohio
SAM BROWNBACK, Kansas
WAYNE ALLARD, Colorado

ROBERT C. BYRD, West Virginia
DANIEL K. INOUYE, Hawaii
PATRICK J. LEAHY, Vermont
TOM HARKIN, Iowa
BARBARA A. MIKULSKI, Maryland
HARRY REID, Nevada
HERB KOHL, Wisconsin
PATTY MURRAY, Washington
BYRON L. DORGAN, North Dakota
DIANNE FEINSTEIN, California
RICHARD J. DURBIN, Illinois
TIM JOHNSON, South Dakota
MARY L. LANDRIEU, Louisiana

J. KEITH KENNEDY, *Staff Director*
TERRENCE E. SAUVAIN, *Minority Staff Director*

SUBCOMMITTEE ON THE DEPARTMENT OF HOMELAND SECURITY

JUDD GREGG, New Hampshire, *Chairman*

THAD COCHRAN, Mississippi
TED STEVENS, Alaska
ARLEN SPECTER, Pennsylvania
PETE V. DOMENICI, New Mexico
RICHARD C. SHELBY, Alabama
LARRY CRAIG, Idaho
ROBERT F. BENNETT, Utah
WAYNE ALLARD, Colorado

ROBERT C. BYRD, West Virginia
DANIEL K. INOUYE, Hawaii
PATRICK J. LEAHY, Vermont
BARBARA A. MIKULSKI, Maryland
HERB KOHL, Wisconsin
PATTY MURRAY, Washington
HARRY REID, Nevada
DIANNE FEINSTEIN, California

Professional Staff
REBECCA DAVIES
JAMES HAYES
CAROL CRIBBS
KIMBERLY NELSON HILL
SHANNON O'KEEFE
CHARLES KIEFFER *(Minority)*
CHIP WALGREN *(Minority)*
SCOTT NANCE *(Minority)*
DRENAN E. DUDLEY *(Minority)*

Administrative Support
AVERY FORBES

CONTENTS

WEDNESDAY, MARCH 2, 2005

	Page
Department of Homeland Security	1

WEDNESDAY, APRIL 20, 2005

Department of Homeland Security	117

THURSDAY, APRIL 28, 2005

Department of Homeland Security	349
Nondepartmental Witnesses	435

DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR FISCAL YEAR 2006

WEDNESDAY, MARCH 2, 2005

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10:34 a.m., in room SD–138, Dirksen Senate Office Building, Hon. Thad Cochran presiding.

Present: Senators Cochran, Byrd, and Leahy.

DEPARTMENT OF HOMELAND SECURITY

STATEMENTS OF:

MICHAEL J. GARCIA, ASSISTANT SECRETARY, IMMIGRATION AND CUSTOMS ENFORCEMENT

ROBERT C. BONNER, COMMISSIONER, CUSTOMS AND BORDER PROTECTION

EDUARDO AGUIRRE, JR., DIRECTOR, U.S. CITIZENSHIP AND IMMIGRATION SERVICES

STATEMENT OF SENATOR THAD COCHRAN

Senator COCHRAN. The hearing will please come to order. Today we begin our committee's review of the fiscal year 2006 budget request for the Department of Homeland Security. We will consider specifically the request for programs and activities of U.S. Citizenship and Immigration Services, Customs and Border Protection, and Immigration and Customs Enforcement.

I am pleased to welcome the Director of U.S. Citizenship and Immigration Services, Eduardo Aguirre; the Commissioner of Customs and Border Protection, Robert Bonner; and the Assistant Secretary of Immigration and Customs Enforcement, Michael Garcia.

Our committee will work with you to help ensure that we provide the funds necessary for your agencies to carry out their responsibilities and missions. For fiscal year 2006, the President's budget requests $12.9 billion to fund the organizations appearing before us today. This includes mandatory and discretionary appropriations, user fee collections, and trust funds.

We thank each of you for submitting to the committee copies of your statements in advance. These will be made a part of the record and we invite you to make any comments you think will be helpful to the committee's understanding of the budget request.

Before hearing from the witnesses, I am pleased to yield to Senator Leahy or other Senators who may wish to make opening statements. Senator Leahy.

STATEMENT OF SENATOR PATRICK J. LEAHY

Senator LEAHY. Thank you, Mr. Chairman.

I think these three agencies before us have the duty of keeping our Nation safe, but also keeping our historic commitment to legal immigration. I know I have to think about the fact that my grandparents came, my maternal grandparents, came to this country not speaking any English. If they had not been here, their grandson would not be here, and how proud and how happy they were to come.

I remember talking with my grandparents as a child and how much it meant to them to be the first generations of Americans. It has left a mark in my own mind. You look around this room, look around anywhere else, look at your own backgrounds, and we know that we are a Nation of immigrants. We have to keep being able to do that.

BUDGET SHORTFALLS AND INCREASED STAFFING FOR THE BORDER PATROL

When we held hearings on these three agencies last year, Mr. Chairman, they were facing substantial budget shortfalls. They had imposed hiring freezes. I want to know where we stand today on these issues. I am concerned that the administration is ignoring Congress's clear and consistent call, call from both Republicans and Democrats, for substantial increases in staffing for the Border Patrol. The Border Patrol's presence on our northern border—and I want to remind everybody we have a northern border as well as a southern border; I live an hour's drive from it—it was minimal before the September 11th attacks. I think we had something like 300 agents stretched over 4,000 miles of border. There is no other place in the world similar to that.

I authored a provision in the Patriot Act to triple that number. It has been achieved. A lot more needs to be done. The President signed the Intelligence Reform and Terrorism Prevention Act of 2004. That mandated increasing at least 2,000 Border Patrol agents for fiscal year 2006, 20 percent of them for the northern border. But that is the good news and the President did sign that bill for the 2,000, but his budget provides only enough funding for 210. So he signed the bill with great fanfare for 2,000 and put the budget in for 10 percent of it. And it appears none of them go to the northern border.

So I hope Mr. Bonner will explain why the administration is not heeding this Congressional mandate and whether he now believes it is time to declare mission accomplished for the job of protecting our northern border.

LAW ENFORCEMENT SUPPORT CENTER

Assistant Secretary Garcia and I have spoken a number of times about the excellent work of the Law Enforcement Support Center. We have visited this. This is the place that stores information for State and local police. It provides immigration status and identities of aliens any time of the day or night, every day of the year.

FISCAL YEAR 2006 BUDGET REQUEST FOR CITIZENSHIP AND IMMIGRATION SERVICES

Of course, Mr. Aguirre, we talked before, I am concerned about the President's proposed budget for Citizenship and Immigration Services. It calls for a 50 percent cut in the amount of directly appropriated funds for CIS. At the same time the President says he will achieve his goal of reducing the average wait time for applicants for immigration benefits to 6 months.

He has asked the Congress to enact a guest worker program that is going to significantly increase the CIS workload. That is fine, we can increase it, but if the administration is cutting the manpower for this substantially, but wanting to add to the workload, I do not know how you ever get here.

H2B VISA PROGRAM

I hope—the last thing is I hope the CIS and the administration will support bipartisan efforts in Congress to increase the cap for the H2B visa program. The Department announced in January for the second straight year the statutory cap has been reached and that is causing tourism-related businesses across the country to go into justifiable panic and concern.

We have a bipartisan group of 16 colleagues introducing S. 352, the Save Our Small and Seasonal Business Act of 2005. It would allow aliens who obtained H2B visas in recent years to reenter under that program. I hope the administration would support it. It is a quick, easy, I think effective, cost effective way of handling this.

So thank you, Mr. Chairman. Those are some of the concerns I have. I thought I would express them here because I know we are going to have votes in between and I may have to go back and forth.

Senator COCHRAN. Thank you very much, Senator.

Senator Byrd.

STATEMENT OF SENATOR ROBERT C. BYRD

Senator BYRD. Thank you, Mr. Chairman.

Excuse me, I am sorry.

Senator LEAHY. Any time you want.

Senator BYRD. Thank you.

Well, today, Mr. Commissioner and also Mr. Assistant Secretary and Director Aguirre, we hold the first hearing on the President's budget for the Department of Homeland Security. Chairman Cochran and I have worked together over the last 2 years to produce bipartisan legislation to fill critical gaps in the security of our homeland. I commend Chairman Thad Cochran for his excellent leadership of this subcommittee and of any other committee or subcommittee that he chairs. I know how well it is going to be run.

Today our witnesses will focus on issues related to border security, immigration, and trade. For the third year in a row, the President has submitted a budget for the Department of Homeland Security that ignores the stark reality of the resources needed to secure the homeland. The 9/11 Commission report concluded this:

"More than 500 million people annually cross U.S. borders at legal entry points, about 330 million of them non-citizens." What a flow of humanity. "Another 500,000 or more enter illegally without inspection across America's thousands of miles of land borders or remain in the country past the expiration of their permitted stay." Now, that was the commission talking.

The commission concluded that, quote: "Two systemic weaknesses came together in our border system's inability to contribute to an effective defense against the 9/11 attacks: one, a lack of well-developed counterterrorism measures as a part of border security; and two, an immigration system not able to deliver on its basic commitments, much less support counterterrorism."

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT

In response to the commission's findings, Congress enacted the Intelligence Reform and Terrorism Prevention Act. In a December 6, 2004, letter to the Congress urging final passage of that Act, President Bush stated, "I also believe the conference took an important step in strengthening our immigration laws by, among other items, increasing the number of Border Patrol agents and detention beds." Close of quotation.

As enacted, the Act authorizes the hiring of 2,000 new Border Patrol agents and 800 new ICE investigators and the funding of 8,000 new detention beds for illegal alien immigrants. Yet, when the President submitted his budget request months after sending that letter, virtually no new funds were requested for any of these activities.

At the same time, the President's own terrorism experts are extremely concerned about the threat posed by terrorists to our borders. In written testimony before the Senate Intelligence Committee on February 16, 2005, the Department's Deputy Secretary, Admiral James Loy, cited recently received information as the reason for his concern about the threat facing the Mexican border. He called it a "very serious situation" and added: "Several Al Qaeda leaders believe operatives can pay their way into the country through Mexico and also believe illegal entry is more advantageous than legal entry." How about that, "believe illegal entry is more advantageous than legal entry for operational security reasons."

FUNDING ISSUE

Despite this testimony, there is virtually no funding in the budget to increase our border security. In addition to having a strong deterrent to illegal immigration at the border, it is critically important for the Department to have the resources to enforce our immigration laws. Therefore, I am very troubled by the fact that 6 months into the fiscal year we have not received a supplemental request or a reprogramming proposal to address a shortfall in funding for immigration and customs enforcement.

Since last spring, the Congress has been ringing the alarm bell—ding-a-ling, ding-a-ling, ding-a-ling—that the Department's primary investigative arm, Immigration and Customs Enforcement, ICE, faced significant budget shortfalls. To partially address this problem, ICE last year instituted a hiring freeze, significantly reduced spending, and took other painful steps—bring on the aspi-

rin—to cope with the shortfall. There were even media reports that some apprehended illegal aliens were being released because ICE could not afford to cover the costs associated with holding these individuals.

Well, Congress stepped up to the plate. This man, Cochran, he is on the ball. Congress stepped up to the plate by providing ICE with $193 million more for the current fiscal year than requested by the President. However, the hiring freeze and other spending restraints remain in place halfway through the new fiscal year. We are being warned by the Department that ICE faces a funding gap of nearly $300 million for the rest of this year.

Has the President found any room in his $81.9 billion supplemental spending request to address this gap? No. He is willing to request billions of dollars for foreign aid to build the most expensive U.S. embassy in the world in Baghdad. I do not plan to go there often. But he does not seem to be able to find the funds to hire and support the men and women fighting the war on terrorism here at home.

Today I sent a letter to Secretary Chertoff raising these issues, and I hope that he will work with the White House to send to the Congress a request that would implement the recommendations of the 9/11 Commission contained in the Intelligence Reform and Terrorism Prevention Act.

Thank you, Mr. Chairman. Thank you, Mr. Commissioner.

[The information follows:]

LETTER FROM SENATOR ROBERT C. BYRD

U.S. SENATE,
Washington, DC, March 2, 2005.

Hon. MICHAEL CHERTOFF,
Secretary, Department of Homeland Security,
Washington, DC.

DEAR SECRETARY CHERTOFF: Congratulations are in order as you assume the task of leading the Department of Homeland Security, an immense and important burden. Sadly, the President, in his fiscal year 2006 budget request for the Department, has not made your task any easier.

For the third year in a row, the President has submitted a budget that ignores the stark reality of the steps needed to secure the homeland.

The 9/11 Commission report concluded that:

More than 500 million people annually cross U.S. borders at legal entry points, about 330 million of them noncitizens. Another 500,000 or more enter illegally without inspection across America's thousands of miles of land borders or remain in the country past the expiration of their permitted stay. The challenge for national security in an age of terrorism is to prevent the very few people who may pose overwhelming risks from entering or remaining in the United States undetected.

Our investigation showed that two systemic weaknesses came together in our border system's inability to contribute to an effective defense against the 9/11 attacks: a lack of well-developed counterterrorism measures as a part of border security and an immigration system not able to deliver on it basic commitments, much less support counterterrorism.

In response to the Commission's findings, Congress enacted the Intelligence Reform and Terrorism Prevention Act. In his December 6, 2004, letter to Congress urging final passage of that Act, President Bush stated, "I also believe the Conference took an important step in strengthening our immigration laws by, among other items, increasing the number of border patrol agents and detention beds." As enacted, the Act authorizes the hiring of 2,000 new Border Patrol agents and 800 new ICE investigators, and the funding of 8,000 new detention beds for illegal aliens immigration. The President's letter called that "an important step." Yet that letter appears to be another empty rhetorical gesture. When the President submitted his

budget request 2 months after sending that letter, virtually no new funds were requested for any of these activities.

At the same time, the President's own terrorism experts are extremely concerned about the threat terrorists pose to our borders. In written testimony before the Senate Intelligence Committee on February 16, 2005, the Department's Deputy Secretary, Admiral James Loy cited recently received information as the reason for his concern about the threat facing the Mexican border. He called it a "very serious situation" and added, "several Al Qaeda leaders believe operatives can pay their way into the country through Mexico and also believe illegal entry is more advantageous than legal entry for operational security reasons."

Mr. Secretary, I know that this budget was completed prior to your coming onboard. I strongly encourage you to work with the White House to formally request additional resources to implement the Intelligence Reform and Terrorism Prevention Act authorization enacted to respond to the recommendations of the 9/11 Commission.

In addition to having a strong deterrent to illegal immigration at the border, it is critically important for the Department to have the resources to enforce our immigration laws. Therefore, I am very troubled by the fact that, 6 months into the fiscal year, we have not received a supplemental request or reprogramming proposal to address a shortfall in funding for Immigration and Customs Enforcement. Since last spring, the Congress has been ringing the alarm bells that the Department's primary investigative arm, Immigration and Customs Enforcement (ICE), faced significant budget shortfalls. To partially address this problem, ICE last year instituted a hiring freeze, significantly reduced spending, and took other painful steps to cope with the shortfall. There were even media reports that some apprehended illegal aliens were being released because ICE could not afford to cover the costs associated with holding these individuals.

Congress stepped up to the plate by providing ICE with $193 million more for the current fiscal year than requested by the President. However, the hiring freeze and other spending restraints remain in place halfway through the new fiscal year. We are being warned by the Department that ICE faces a funding gap of nearly $300 million for the rest of this year. Has the President found any room in his $81 billion supplemental spending request to address this gap? No. He is willing to add to the deficit to provide hundreds of millions of dollars to build the most expensive U.S. embassy in the world in Baghdad, but he does not seem to be able to find the funds to hire and support the men and women fighting the war on terrorism here at home. To them, he suggests they carpool to work.

Mr. Secretary, you really have your work cut out for you. Our repeated entreaties to the President and his representatives to provide the resources to meet these threats fall on deaf ears. I know that you will do all that you can to get this Administration to put its money where its rhetoric is. I wish for you success.

With kind regards, I am.

Sincerely yours,

ROBERT C. BYRD,
U.S. Senator.

Senator COCHRAN. Thank you, Senator Byrd.

STATUS OF SECURITY OF THE UNITED STATES 2 YEARS AFTER THE ESTABLISHMENT OF THE DEPARTMENT OF HOMELAND SECURITY

I am going to ask our witnesses, in view of the fact that it has been almost exactly 2 years—March 1, 2005, actually would have been the second anniversary of the establishment of the Department of Homeland Security—in your estimation from what you know as administrators of these important agencies at the Department, are we safer now 2 years later after the Department of Homeland Security has been created than we were 2 years ago?

Mr. Garcia, would you like to start?

Mr. GARCIA. Thank you very much, Mr. Chairman. That is a question I often hear in many different forms, and everybody brings I think their own perspective.

Senator COCHRAN. I am going to ask each one to answer that before you proceed with your statements. Tell us what you think?

ICE RESPONSE

Mr. GARCIA. I think we are safer, yes, and I bring perspective I think that is somewhat unique to that answer. I was a prosecutor in New York in the 1990s. I prosecuted many of the terrorism cases before 9/11 and I saw terrible exploitation of our immigration systems and our border security in those cases. Now, as part of the Homeland Security Department, I am a piece of the Government's response to those attacks in a Department that was created to address the vulnerabilities that were exposed by the 9/11 attacks.

From that vantage point, I can clearly say that we are safer, and I see evidence of that, Mr. Chairman, every day. I will speak mostly about the ICE contributions here and how my agency has responded with creativity, using these new combined authorities that we have been given in ICE. You look at the systems and we have created—and I think Senator Leahy and Senator Byrd may have mentioned—overstays and how there was no tracking. We have created a Compliance Enforcement Unit that sends out thousands of prioritized leads to look at deterrent effect, to look at enforcing our immigration rules and bringing integrity to the system as a whole.

We work very hard in benefits fraud with Director Aguirre's folks to close those vulnerabilities that were exploited in the past. So we are improving the integrity of the system.

Senator COCHRAN. Let me ask Mr. Bonner for his reaction to that question before you proceed with your full statement.

CBP RESPONSE

Mr. BONNER. Yes, thank you, Mr. Chairman. First of all, yes, America is absolutely unquestionably safer now than it was before the creation of the Department of Homeland Security on March 1, 2003. Our borders are more secure now than they were before 2001—excuse me, March 1, 2003. Part of that is that one of the truly big and important ideas of the Department of Homeland Security was to create one front-line border agency for our government that combined at our front line all of Customs' powers and personnel, Immigration powers and personnel, agriculture protection, and most importantly anti-terrorism as a focus and a priority mission.

So as a result of that one step alone, unifying our border agencies, whereas before March 1, 2003, they had literally been fragmented at our borders, at our ports of entry, among four different agencies of government reporting to three different Departments, it is now one front-line border agency, that is Customs and Border Protection, within the Department of Homeland Security, with a priority mission which is nothing less than keeping terrorists and terrorist weapons out of our country.

So are we totally safe? No, but we are safer and more secure because our borders are more secure.

Senator COCHRAN. Mr. Aguirre.

USCIS RESPONSE

Mr. AGUIRRE. Mr. Chairman, as the Director of the agency that is responsible for administering immigration services, I say unquestionably we are safer from the vantage point in which I sit. We

process 6 to 7 million applications a year and we have implemented some national security components and fraud deterrent components that were simply not there 2 or 3 years ago. Therefore I think we have tightened the filter, if you will, to determine those who may do us harm or who wish to take advantage of our good nature. I think we are much better off.

There is no finish line to this effort, but I think we are far, far beyond where we were a couple years ago.

Senator COCHRAN. Thank you very much.

Now you may proceed with your opening statements. Mr. Garcia?

STATEMENT OF MICHAEL GARCIA

Mr. GARCIA. Mr. Chairman, Senator Byrd, Senator Leahy, it is my pleasure to be with you today to discuss the President's fiscal year 2006 budget request for U.S. Immigration and Customs Enforcement, or ICE, the largest investigative arm of the Department of Homeland Security. The $4.36 billion request underscores the vital role that ICE plays in the Department's mission of ensuring the security of the American people.

In order to provide a better understanding of the President's 2006 budget request for ICE, I would like to first provide you with the context in which the request is made. Specifically, I would like to share with you a few highlights of significant ICE achievements as well as some of the challenges we have faced.

SIGNIFICANT ICE ACHIEVEMENTS

ICE removed a record number, 160,000, illegal aliens from the United States in 2004. More than half of those were criminal aliens. We also arrested a record number of fugitive aliens. In fact, that was an increase of more than 100 percent.

ICE conducted 7,600 money-laundering and other financial investigations. ICE agents conducted more than 2,500 investigations into illegal exports that would have sent sensitive technology and weapons components to Iran, Iraq, China, and other nations. ICE arrested more than 5,000 sexual predators since Operation Predator was launched and have removed almost half of them from the United States. ICE agents also made the first 11 arrests for child sex tourism, targeting U.S. citizens who attempt to exploit children overseas.

ICE arrested more than 1,600 human smugglers and ICE's Federal Protective Service officers made more than 4,000 arrests, a nearly 60 percent increase over the previous year. ICE Federal Air Marshals logged millions of miles on tens of thousands of flights and Air Marshals have completed advanced training, an important benchmark to ensure professionalism and peak performance.

Senator Leahy mentioned the Law Enforcement Support Center in Vermont. That Center received more than 600,000 inquiries from Federal, State, and local law enforcement officials last fiscal year, a 12 percent increase over the year before. 15,000 detainers with police agencies nationwide on aliens were lodged from Vermont alone.

I could continue with many, many additional examples of achievements that ICE's employees have made. I would like to note that ICE's accomplishments over the last 2 years, which I believe

are unprecedented in law enforcement, were brought about despite significant challenges. In addition to the challenges faced in creating a new law enforcement agency, ICE has faced severe budget issues related to resource allocations. During the organization of the new Department, the budgets for component agencies, including those for overhead, information technology support, legal support, and other administrative functions, were broken apart in ways that were not entirely consistent. As a result, in some cases ICE was paying for services when the funds for those services had been allocated to other agencies.

BUDGET ISSUES

When we realized the budget issues that would arise from these allocation errors, we took swift action. ICE placed a freeze on new hires. We limited expenditures to those deemed mission essential and we moved to set clear priorities for funding. We also worked with the Department to undertake a budget review to determine what money was appropriately due to ICE in return for shared services.

These measures got results. Diligent and conscientious efforts on the part of our employees and field management helped us to realize tens of millions of dollars in short-term savings during fiscal year 2004. In addition, ICE identified and recouped more than $500 million from other agencies in the second half of 2004. ICE also bought services from other DHS components as part of the shared services concept, such as human resources, logistics, and fleet management.

We are also in the process of systematically improving financial management throughout the entire agency. Some changes have been implemented and we expect to implement additional improvement in the coming months. These steps have been further outlined in a letter recently submitted to this committee.

COMMUNICATION WITH ICE EMPLOYEES

While this has been a challenging time for ICE, we have made every effort to communicate the facts to our employees at every opportunity through such measures as town hall meetings, broadcast messages to all employees, and visits by myself and other senior members of the agency's leadership to all of our field offices.

Over the past 2 years, ICE employees have refused to be defined by our challenges, but rather we have been defined by our achievements, which represent the true story of our agency. Our accomplishments represent the abiding commitment of all ICE employees to meeting these challenges head-on and accomplishing the critical mission with which we are charged.

FISCAL YEAR 2006 BUDGET REQUEST

The proposed 2006 budget builds on the foundation of our accomplishments while addressing many of the challenges outlined above. The President's 2006 budget request seeks more than $4.36 billion for ICE, which represents an increase of more than 13 percent over fiscal year 2005. I would like to briefly address these enhancements.

DETENTION AND REMOVAL

The President's 2006 budget proposal request seeks $176 million in enhancements for Detention and Removal operations. These enhancements will be used to fund detention bed space and management, Alternatives to Detention, Fugitive Operations, the Institutional Removal Program and interior repatriation. This funding will help ICE to continue to build on the vigorous enforcement efforts we have developed in the last 2 years.

INVESTIGATIONS AND INTELLIGENCE

The President's budget also seeks $171 million in enhancements for ICE investigations and intelligence. Specifically, the budget will replace funding for Organized Crime Drug Enforcement Task Force activities. This enhancement requests no additional positions or money, but proposes that 346 positions currently on board be paid by direct appropriation instead of reimbursement from DOJ. In addition to a base increase, the enhancement allows for maintenance of Visa Security operations initiated in 2005 and support for one additional Visa Security Unit overseas. It funds 143 positions and training to successfully implement a worksite enforcement component for the proposed temporary worker program.

FEDERAL AIR MARSHALS SERVICE

We are also seeking enhancements to increase staffing for the Federal Air Marshal Service, funding for additional attorneys required to improve the ability of ICE's legal program to complete matters in Immigration Court, and money for Department-wide secure classified and computer to computer connectivity.

OVERVIEW OF ICE FISCAL YEAR 2006 BUDGET REQUEST

The President's 2006 budget request for ICE is a solid step forward for this agency and ICE is dedicated to protecting the homeland by enforcing immigration and customs laws, restoring integrity to the immigration system, as we discussed before, and ensuring the sanctity of our financial and trade systems. We protect Federal property and we ensure the security in our civil aviation.

That is a broad and diverse mission, but the men and women of ICE are dedicated to building this agency into a model for law enforcement in the 21st century. The 2006 budget request provides us with the resources that will make this goal a reality as we strive to secure the American homeland and protect the American people.

PREPARED STATEMENT

I would like to thank you, Mr. Chairman, Senator Byrd, Senator Leahy, for the opportunity to testify before you today. I look forward to answering any questions you may have.

[The statement follows:]

PREPARED STATEMENT OF MICHAEL J. GARCIA

INTRODUCTION

Mr. Chairman, Senator Byrd, and distinguished Members of the Subcommittee. It is my pleasure to be with you today to discuss the President's fiscal year 2006

budget request for U.S. Immigration and Customs Enforcement (ICE), the largest investigative arm of the Department of Homeland Security (DHS). This $4.36 billion request underscores the vital role that ICE plays in the Department's mission of ensuring the security of the American people.

By integrating these various components in a single agency, ICE is able to more effectively meet the threats of the post-9/11 world, wherever these threats may arise—across our borders, within the Nation's interior, in our financial systems, at Federal facilities nationwide, in cyberspace, or civil aviation.

With ICE's broad authorities and expertise, we are prepared to counter the threats posed by criminal and terrorist organizations in ways not possible before the creation of the Department of Homeland Security.

REVIEW OF ICE ACCOMPLISHMENTS

In order to provide a better understanding of the President's fiscal year 2006 budget request for ICE, I would first like to provide you with the context in which the request is made. Specifically, I would like to share with you a few highlights of significant ICE achievements as well as some of the challenges we have faced.

—*Prioritizing Removals of Criminal and Fugitive Aliens.*—As part of our mission to restore integrity to the Nation's immigration system, the Office of Detention and Removal Operations (DRO) removed a record number of illegal aliens from the United States, posting approximately 160,200 such removals. More than half of those were criminal aliens. 7,200 fugitive aliens were removed last fiscal year—an increase of 112 percent over the previous year.

—*Protecting U.S. Financial and Trade Systems.*—The ICE Office of Investigations conducted 7,670 money laundering and other financial investigations in fiscal year 2004, resulting in more than 1,368 arrests, 895 indictments and the seizure of more than $202 million. These achievements stem from ICE's Cornerstone initiative, in which we direct our expertise in financial, trade, and intellectual property investigations toward shutting down the schemes that criminal or terrorist organizations use to earn, move, and store their assets.

—*Checking Illegal Flows of Weapons and Sensitive Technology.*—ICE agents conducted more than 2,500 investigations into the illegal export of U.S. arms and technology in fiscal year 2004. These investigations protect national security by keeping sensitive technologies and weapons—whether it's missile components or night vision technology, laser scopes for military rifles or sensitive software—out of the hands of our Nation's adversary. In the last year, ICE investigated export violations that would have sent sensitive technology and weapons components to Iran, Iraq, China, and other nations. These investigations not only contribute to the security of the United States, but they serve to enhance the security of our troops and allies around the globe as well.

—*Protecting Children from Sexual Exploitation.*—Under Operation Predator, ICE arrested more than 4,900 sexual predators since the program was launched in 2003. We have ensured that 2,100 of those predators were removed from the United States. ICE agents also made the first 11 arrests for child sex tourism, targeting U.S. citizens who attempt to exploit children overseas under the PROTECT Act. Leads developed out of ICE investigations into online child pornography have been provided to foreign law enforcement authorities through ICE's 54 International Attaché offices. These leads have led to the arrest of approximately 850 child pornography subscribers overseas. ICE Attaches also provided expertise and support to their law enforcement counterparts in areas ravaged by the tsunami waves in southeast Asia in December, to ensure that children were not victimized by sexual predators or trafficking networks.

—*Targeting Human Smuggling and Trafficking.*—Another of ICE's top priorities is to dismantle criminal organizations that smuggle and traffic human beings for profit. In fiscal year 2004, ICE arrested more than 1,630 human smugglers. Operation ICE Storm, an initiative we launched in 2003 to target violent human smuggling networks in Arizona, has brought charges against more than 300 defendants and resulted in the seizure of more than $7 million. This unprecedented seizure of alien smuggling proceeds is a direct result of the combination of our immigration and customs authorities (particularly customs financial crimes expertise). Law enforcement authorities in Arizona have credited Operation ICE Storm with a dramatic decrease in homicides and other violent crime in the Phoenix metropolitan area.

—*Improving Security at Federal Facilities.*—ICE's Federal Protective Service (FPS) made 4,426 arrests in fiscal year 2004—a 58 percent increase over the previous fiscal year. In addition, FPS officers prevented nearly 550,000 prohibited items and weapons from being carried into Federal facilities—a fourfold in-

crease over the previous year. FPS officers also responded to 430 bomb threats and more than 875 calls about suspicious packages and other items. All of these achievements are key components of the FPS mission to provide a safe and secure environment for Federal workers and the American public.

—*Enhancing Security in the Skies.*—ICE's Federal Air Marshal Service (FAMS) once again logged millions of miles on tens of thousands of flights in fiscal year 2004, as part of the division's enhanced mission of providing security in the air since 9/11. All FAMS recruited and deployed since 9/11 have successfully completed advanced training—an important benchmark to ensure professionalism and peak performance.

—*Stopping the Flow of Drugs into the United States.*—ICE plays a leading role in the Nation's war on drugs, with significant results. In fiscal year 2004, ICE agents, working in cooperation with our partners at other agencies, were involved in the seizure of roughly 3.1 million pounds of illegal drugs in fiscal year 2004—a 63 percent increase over the previous year. Another key achievement stemming from an ICE investigation was the extradition of one of the leaders of Cali drug cartel from Colombia, as well as the arrest of several leaders of the Norte Valle cartel.

—*Providing Support and Assistance to the Law Enforcement Community.*—ICE's Law Enforcement Support Center (LESC) responded to more than 603,000 inquiries related to immigration status from Federal, State, and local authorities in fiscal year 2004—a 12 percent increase over the previous year. In addition, the LESC placed more than 15,000 immigration detainers with police agencies nationwide. These detainers allow ICE to more efficiently remove aliens from the United States once their jail term is expired.

CHALLENGES

I could continue with many, many additional examples. I would like to note that ICE's accomplishments of the last 2 years—which I believe are unprecedented in law enforcement—have taken place against a backdrop of significant challenges.

First, we have faced the organizational and logistical challenges inherent in bringing our various divisions together into an integrated whole within the Department of Homeland Security. The challenges of the DHS reorganization have been likened to "trying to change the engine in an airplane in mid-flight." We have certainly experienced those challenges at ICE, where we have had to build a new agency almost from the ground up—bringing together divisions from four separate agencies into a single functioning unit, and melding the cultures and missions of various units into a unified whole. This process was analogous to that of building a new start-up company while performing a large-scale merger and acquisition—with the notable difference that we had but a few weeks to accomplish our merger, compared to the months, or years, that would be devoted to a merger in the private sector. While the reorganization is still ongoing, I am pleased to report that the majority of these organizational and logistical challenges have been met and addressed, thanks to the commitment, and perseverance of ICE employees.

Another significant challenge that ICE has faced has been budget issues related to resource allocations. During the reorganization of the new department, the budgets for component agencies—including those for overhead, information technology support, legal support, and other administrative functions—were broken apart in ways that were not entirely consistent. As a result, in some cases ICE was paying for services when the funds for those services had been allocated to other agencies. When we realized the budget issues that would arise from these allocation errors, we took swift action. ICE placed a temporary freeze on new hires; we limited expenditures to those deemed "mission essential"; and we moved to set clear priorities for funding. We also worked with DHS to undertake a budget review to determine what money was appropriately due to ICE in return for shared services.

These measures got results. Diligent and conscientious efforts on the part of our employees and field management helped us to realize $120 million in short-term savings during fiscal year 2004. In addition, ICE identified and recouped more than $500 million from other agencies in the second half of fiscal year 2004. ICE also bought services from other DHS components as part of the shared services concept such as HR, logistics and fleet management.

We are also in the process of systematically improving financial management throughout the entire agency. Some changes have been implemented, and we expect to implement additional improvements in the coming months. We will update the Congress periodically with details on our reforms in reports requested by the Committees.

While this has been a challenging time for ICE, we have made every effort to communicate the facts to our employees at every opportunity—through such measures as town hall meetings; broadcast messages to all employees; and visits by myself and other members of the agency's senior leadership to all of our field offices.

Over the past 2 years ICE employees have refused to be defined by our challenges, but rather by our achievements, which represent the true story of our agency. Our accomplishments represent the abiding commitment of all ICE employees to meeting these challenges head-on and accomplishing the critical mission with which we are charged.

BUDGET REQUEST FOR FISCAL YEAR 2006

The proposed fiscal year 2006 budget builds on the foundation of our accomplishments while addressing many of the challenges outlined above. The President's fiscal year 2006 Budget request seeks more than $4.36 billion for ICE, which represents an increase of 13.5 percent over fiscal year 2005. This budget request will allow ICE to pursue our priority missions—including the apprehension, detention, and removal of illegal aliens; financial and trade investigations; protection of Federal infrastructure; and protection of the civil aviation system—with even greater effectiveness. In my testimony, I will address our major program areas—Investigations, Detention and Removal Operations, the Federal Air Marshal Service, and the Federal Protective Service—as well as issues related to management, administration, and information technology.

FISCAL YEAR 2006 ENHANCEMENTS

The President's fiscal year 2006 budget proposal request for ICE Detention and Removal Operations will enhance public safety and national security by ensuring that those aliens who pose the most critical threats are removed from the United States first—a critical objective in ICE's long-term strategy to restore integrity to the Nation's immigration system. In addition, this funding will help ICE to meet its detention needs, which are growing every year as we move to aggressively enforce immigration laws. This funding will help ICE to continue building on the vigorous enforcement efforts we have developed in the last 2 years.

Detention and Removal Operations.—The DHS Immigration and Customs Enforcement (ICE) fiscal year 2006 President's budget seeks $176.0 million in enhancements for Detention and Removal Operations:

—$90 million/16 Full-Time Employees (FTEs) for Custody Management/Bedspace. In many cases, apprehended aliens must be detained while they go through immigration proceedings and until they are removed. Custody Management provides safe, secure, and humane confinement for these aliens. It also ensures that aliens in ICE custody appear for their immigration hearings, and then for their subsequent removal. This request would provide $90 million to fund requirements of the Custody Management budget activity, adding 16 FTE and increasing funded bedspace by 1,920 beds. This enhancement will improve detention efforts that ensure public safety and national security.

—$5.4 million/7 FTEs for the Alternatives to Detention program. The Alternatives to Detention program places low-risk aliens under close supervision, rather than into traditional detention, serving as a cost-effective way to ensure their appearance for an immigration hearing or for removal. ICE's Intensive Supervision Appearance Program (ISAP) is a community-based case management program that is aimed at improving the appearance rate of aliens at immigration hearings. This request includes $5.4 million/7 FTE to expand the ISAP to two additional locations.

—$8.9 million for Fugitive Operations. Approximately 465,000 aliens have received final orders of removal but are not confirmed to have departed the United States. This request includes $8.9 million to enhance case management resources that enable the Fugitive Operations program to locate and apprehend fugitive aliens in the United States. This investment will serve to improve the integrity of the immigration enforcement process that is instrumental in deterring the efforts of potential absconders.

—$5.4 million/19 FTEs for the Institutional Removal Program (IRP). Many removable aliens are currently incarcerated in Federal or State prisons for criminal convictions. If these aliens are released upon completion of their criminal sentence, they are likely to avoid immigration removal proceedings. The IRP ensures that these aliens are not released back into the community before they are removed from the United States. The $5.4 million requested would provide for Immigration Enforcement Agents to enhance the IRP with staff support

needed to facilitate the removal of aliens following completion of criminal sentences.

—$39.3 million for Interior Repatriation, as part of the Arizona Border Control multi-agency effort. One of the major components of enhanced border control is a focus on border safety through the removal of migrants from the dangers associated with crossing the border illegally. The United States, in cooperation with the government of Mexico, has focused on the use of every available tool to break the cycle of migrant deaths in the dangerous terrain where human smugglers value profits more than the human life they often sacrifice for personal gain. One of the major tools agreed to by both countries is the use of a voluntary interior repatriation program. The interior repatriation program allows for movement at the U.S. border of Mexican nationals who voluntarily return to selected cities within the interior of Mexico by means of commercial flights. Without this program, a significant number of persons who are apprehended and returned to Mexico at the border seek re-entry through dangerous border terrains, thus repeatedly risking injury or death in the process.

—$24.0 million for the Office of Detention and Removal. This request provides that the base budget for Detention Removal Operations be adjusted by $24 million for salary costs and operating expenses. These funds will augment support for increased detention and removal activities to ensure the departure of removable aliens from the United States through the fair enforcement of immigration laws.

ICE's Office of Investigations and Office of Intelligence play a vital role in advancing national security and homeland defense through aggressive investigations and cooperation with other agencies to share information on organized criminal activity and terrorist organizations. ICE's investigators have a long history of targeting money laundering networks; narcotics trafficking; criminal financial schemes; counterfeiting and piracy; trade fraud; export violations; and other financial and economic crimes. In addition, our investigators lead the way in targeting child sexual predators, human traffickers, and child labor violators. Our investigators are also at the forefront of combating immigration violations, including enforcement of immigration laws at worksites and shutting down organizations that provide fraudulent documentation for a price.

Investigations and Intelligence.—The ICE fiscal year 2006 President's budget seeks $171.7 million in enhancements for Investigations and Intelligence:

—$43.7 million/346 FTEs for Organized Crime Drug Enforcement Task Force (OCDETF) activities. This increase replaces funding previously received on a reimbursable basis from the Department of Justice (DOJ) for ICE's participation in the OCDETF program. OCDETF is a Federal drug enforcement program that focuses on the disruption and dismantling of major drug trafficking organizations. OCDETF has been in existence since 1982 and operates under the guidance and oversight of the Attorney General. Employing the resources and expertise of 11 member Federal agencies, along with support from State and local law enforcement agencies, OCDETF has contributed to the successful prosecution and conviction of more than 44,000 members of criminal organizations and resulted in the seizure of cash and property assets totaling more than $3.0 billion. This enhancement requests no additional FTEs but proposes that 346 positions currently on board be paid by direct appropriation instead of by reimbursable funding.

—$5.0 million/5 FTEs for Visa Security Program Expansion. The ICE Visa Security Program provides follow-up investigations on visa applicants seeking to enter the United States, for the purpose of denying visas to terrorists, criminals, and persons of special interest. Officers are assigned to posts to perform this law enforcement review of immigrant and nonimmigrant visa applications prior to visa issuance by consular officers of the Department of State. This enhancement would allow ICE to maintain operations initiated in fiscal year 2005 and support one additional Visa Security Unit overseas.

—$18.0 million/72 FTEs for Temporary Worker Worksite Enforcement. As part of the President's proposed temporary worker program (TWP) to match willing foreign workers with willing U.S. employers, enforcement of immigration laws to ensure compliance is required. The requested resources would fund 143 positions and the required training to conduct employer audits, investigate possible violations, and prepare criminal employer case presentations. This funding more than doubles the resources dedicated to the worksite enforcement effort.

—$105.0 million for the Office of Investigations. This request includes $105 million for salary and support costs, including vehicle and other equipment purchases.

—$3.5 million/24 FTEs for Legal Proceedings. This enhancement would provide funding for additional attorneys and support staff required to improve the ability of ICE's legal program to complete matters in Immigration Court and help reduce the case backlog.

—$11.3 million/1 FTE for the Homeland Secure Data Network (HSDN). A total of $37 million is required for the HSDN to provide for secure classified, computer-to-computer connectivity. The HSDN is expected to streamline and modernize the classified data capabilities of DHS to facilitate high-quality and high-value classified data communication and collaboration within DHS and with other Federal agencies and organizations, including the Department of Defense (DOD). Based on modern network and telecommunications designs, the HSDN will optimize both the classified data exchanges between DHS offices, and other networks of classified data such as the Anti-Drug Network (ADNET), Automatic Digital Network (AUTODIN), and Defense Message System (DMS). The HSDN will provide a scalable infrastructure, capable of supporting the growth and evolution of the DHS mission. ICE's allotted portion in support of the network is $11.3 million. Enhancement request includes one position to serve as a liaison between ICE and DHS.

The Federal Air Marshal Service (FAMS) has been charged with providing security in the skies since 9/11. The President's budget request will help FAMS to continue in that mission as we continue the evolutionary process of integrating this key Homeland Security division into the agency.

Federal Air Marshal Service (FAMS).—The ICE fiscal year 2006 President's budget seeks $14.8 million in The Federal Air Marshal Service (FAMS) has been charged with providing security in the skies since 9/11. The President's budget request will help FAMS to continue in that mission as we continue the evolutionary process of integrating this key Homeland Security division into the agency.

Federal Air Marshal Service (FAMS).—The ICE fiscal year 2006 President's budget seeks $9.9 million in enhancements for the Federal Air Marshal Service (FAMS). This enhancement request would allow the FAMS to increase its staffing level to a level that will allow it to meet its mission objective through the risk-based deployment of Federal Air Marshals. In accomplishing this objective, FAMS works closely with DHS and other Federal, State and local agencies and private industry to develop, deploy and sustain a comprehensive intelligence-driven approach and response to terrorist and related criminal threats against the United States and its interests. FAMS provides critical support to the DHS mission to prevent terrorist acts within the United States, reduce vulnerability to terrorism, and minimize damage from potential attacks.

CONCLUSION

The President's fiscal year 2006 budget request for ICE is a solid step forward for the agency. ICE is dedicated to protecting the homeland by enforcing immigration and customs laws; restoring integrity to the immigration system; ensuring the sanctity of our financial and trade systems; protecting Federal property; and ensuring security in the air. That is a broad and diverse mission, but the men and women of ICE are dedicated to building this agency into a model for law enforcement in the 21st century. The fiscal year 2006 budget request provides us with the resources that will make this goal a reality as we strive to secure the American homeland and protect the American people. We look forward to continuing to work with you to accomplish these worthy objectives.

I would like to thank you, Chairman Cochran, Senator Byrd, and Members of the Committee, for the opportunity to testify before you today. I look forward to answering any questions that you may have.

Senator COCHRAN. Thank you very much, Mr. Garcia.

Mr. Bonner, you may proceed.

STATEMENT OF ROBERT C. BONNER

Mr. BONNER. Yes, thank you, Mr. Chairman, Senator Byrd, Senator Leahy. I am very pleased to be here this morning to discuss the fiscal year 2006 budget request for U.S. Customs and Border Patrol, or CBP. I am also very pleased to be here with my colleagues from the Department of Homeland Security, both Director Aguirre of CIS and Mike Garcia, the Assistant Secretary for ICE.

I particularly want to thank the members of this subcommittee for your strong support of the work that CBP does every day 24–7 to protect and defend the borders of our country. As you know, CBP's priority mission is homeland security and for a front-line border agency, which is what we are, that means that CBP's priority mission is keeping terrorists and terrorist weapons from getting into the United States.

The budget request for 2006 in my view will provide resources to perform our all-important priority mission, our anti-terrorism mission, as well as our traditional missions, which go from everything from interdicting illegal drugs at our border to determining admissibility of people appearing at our ports of entry to apprehending people illegally entering the United States, protecting American agriculture, regulating trade, as well as collecting about $27 billion in duties and fees.

FISCAL YEAR 2004 WORKLOAD STATISTICS

The magnitude of our border task is reflected by just a few statistics from fiscal year 2006, because in fiscal year 2004 CBP through its Border Patrol agents apprehended over 1.1 million people illegally entering our country or attempting to enter our country, 1.1 million. By the way, you want to translate that? It is about 3,000 each and every day of the year, day and night.

CBP officers at our ports of entry and Border Patrol agents collectively seized slightly over 2 million pounds, nearly 1 million kilograms, of illegal drugs attempting to be entered through our ports of entry. That is 56,000, by the way, separate seizures of illegal drugs at our borders last year.

We seized almost $46 million in cash and currency that was leaving the United States, much of that of course is from the proceeds of illegal drug trafficking. We just seized about $1.7 million in cash in a vehicle a couple of days ago that was going outbound in a vehicle through the Port of Laredo back to Mexico.

There were 450,000 aliens that were turned around at our ports of entry. By that I mean they were not allowed to enter the United States because they were determined to be inadmissible. There were 78,000 fraudulent passports and other documents that were seized and intercepted by CBP at our borders.

ONE FACE AT THE BORDER

So it gives you an idea of the magnitude of the task, but it also tells you what we are doing and that the job is getting done. We have unified our work force to create one unified front-line border agency for managing and securing and controlling the borders of our country. We have developed a comprehensive border strategy at our ports of entry for our CBP officers and Agriculture specialists and between our ports of entry, primarily our land borders with Mexico and Canada, with our CBP Border Patrol agents.

The transfer of the air and marine operations to CBP last November I believe further strengthens our effort to secure our borders, to interdict drugs at and beyond our borders, and to support our homeland security mission.

TRADE/TRAVEL FACILITATION

We have moved forward on important initiatives set in motion after 9/11 to secure the movement of goods and people across our border and our ports of entry without unduly impeding the legitimate flow of trade, the flow of legitimate trade and travel that is so important to our economy.

WEAPONS OF MASS DESTRUCTION DETECTION TECHNOLOGY

We are also deploying more technology at our ports of entry and between them to help detect potential terrorists and terrorist weapons, including potentially weapons of mass destruction, and I am talking about nuclear devices and radiological weapons, at our borders. This includes, by the way, already the over 400 radiation portal monitors at many of our major ports of entry. We are in phases three and four of that project to deploy better radiation detection equipment at our borders.

As I said, Mr. Chairman, because the personnel and functions from the front-line border agencies of our you have been unified into one border agency, our Nation's borders are more secure and our Nation is safer than it was when we were literally fragmented between four agencies and three different departments of government that were responsible for our border. With over 41,000 approximately FTE Customs and Border Protection, about one-fourth of all the employees of the Department of Homeland Security, is by far the largest actual merger of people and functions taking place in the Department.

COMPREHENSIVE BORDER CONTROL STRATEGY

Having one border agency also allows us for the first time in the history of our country to implement a comprehensive border strategy, not just at our ports of entry but between our ports of entry as well. Between our ports of entry—along the Mexican border and the Canadian border—the strategic goal is clear. That goal is to establish operational control of our borders, which by the way I think was always an important goal for our country, but is absolutely essential, as Senator Byrd suggested in his comments. It is absolutely essential in the post-9/11 era, in the era of global terrorism.

Now, to do this, by the way, it is not all about staffing. It is also about the better use and deployment of technology. It is about organizing ourselves better in terms of how we protect and secure our border. To do this, we have done a number of things that are not widely known. One is we have centralized the Border Patrol command structure and increased the use and deployment of technology, including remote camera system and sensoring devices. We are pioneering as the first law enforcement agency ever the use of unmanned aerial vehicles, or UAV's, to establish literally an aerial patrol over significant segments of our borders.

But we recognize that technology alone, by the way, is not a substitute for well trained and dedicated Border Patrol Agents. One of our goals of our strategy to control the border is to increase our ability to more rapidly deploy Border Patrol Agents to respond to weak spots along our borders with Mexico and Canada.

CARGO/SUPPLY CHAIN SECURITY

Let me just say one other thing. Just shortly after 9/11, U.S. Customs, now CBP, developed a strategy for securing the movement of cargo to the United States and we did that through essentially four interrelated initiatives: the 24-hour rule to get advance information on all cargo coming into the United States; the use of an automated targeting system to identify the high-risk cargo, particularly for the terrorist threat, and that is done at our National Targeting Center in Northern Virginia; the container security initiative, an initiative that partners with other governments to screen high-risk containers before they are loaded on board vessels for the United States. Currently there are 35 foreign seaports that are partnered with us in CIS, including ports like Singapore and Rotterdam, and most recently Shanghai, China.

Through the Customs Trade Partnership Against Terrorism (C–TPAT), our partnership with the private sector, many major importers in the United States, oceangoing carriers and others, to improve the security of the supply chain literally back to the manufacturer, the foreign loading docks of manufacturers in foreign countries, all the way to U.S. ports of arrival, in exchange for benefits of faster processing that CBP can give to goods of companies that have better secured their supply chain.

Those initiatives provide greater protection for our country against potential terrorist attack and not a one of those initiatives existed before 9/11.

PREPARED STATEMENT

Thank you, Mr. Chairman, for letting me make an opening statement and for this opportunity to appear, and I look forward to answering any questions you or the other members may have.

[The statement follows:]

PREPARED STATEMENT OF ROBERT C. BONNER

INTRODUCTION AND OVERVIEW

Chairman Cochran, Ranking Member Byrd, Members of the Subcommittee, it is a privilege and an honor to appear before you today to discuss U.S. Customs and Border Protection's (CBP) fiscal year 2006 budget request.

I want to begin by expressing my gratitude to the Committee for the support it provided for important initiatives implemented by CBP last year. That support enabled CBP to make significant progress in securing our borders and protecting our country against the terrorist threat. As the Commissioner of CBP, I look forward to working with you to build on these successes.

As the frontline border agency, CBP's mission is to prevent terrorists and terrorist weapons from entering the United States. That extraordinarily important priority mission means improving security at our physical borders and ports of entry, but it also means extending our zone of security beyond our physical borders—so that American borders are not our first line of defense.

And we must do this while continuing to perform our traditional missions well. These missions include apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband, protecting our agricultural and economic interests from harmful pests and diseases, protecting American businesses from theft of their intellectual property, regulating and facilitating international trade, collecting import duties, and enforcing U.S. trade laws. In fiscal year 2004, CBP processed almost 30 million trade entries, collected $27 billion in revenue, seized 2.2 million pounds of narcotics, processed 428 million pedestrians and passengers, 121 million privately owned vehicles, and processed and cleared 23.5 million sea, rail and truck containers.

We must perform all of this important security and border-related work without stifling the flow of legitimate trade and travel that is so important to our Nation's economy. In other words, we have "twin goals:" Building more secure and more efficient borders.

The fiscal year 2006 budget for CBP totals $6.7 billion, including $5.6 billion in appropriated resources and $1.1 billion from user fees. The total program increase request for fiscal year 2006 is $261 million. This increase is paramount to help CBP fulfill its priority mission of preventing terrorists and terrorist weapons from entering the United States. As Commissioner, I will continue to ensure funds are devoted to support the traditional missions for which CBP is responsible, including resources for the automation and information technology programs that will improve overall operations of the agency.

Mr. Chairman, although I will touch on each of the priority programs and initiatives in my statement, I want to point out that in many cases, funds spent in one area have a direct and positive impact on other areas. For example, funds spent on automation and information technology provide invaluable assistance to our priority mission of preventing terrorists and terrorist weapons from entering the United States. Also, funds spent on our priority anti-terrorism mission often result in improvements in our effectiveness and efficiency in carrying out our traditional missions, such as interdicting narcotics.

By way of summary of the fiscal year 2006 budget for CBP, I can tell you that the program increases we are requesting include:

—$125 million to continue the deployment and enhancement of Weapons of Mass Destruction Detection Technology to our Nation's ports of entry (POE);
—$19.8 million for the continued deployment of surveillance and intrusion detection technology along our Nation's land borders through the America's Shield Initiative;
—$36.9 million to hire 210 new Border Patrol Agents thereby increasing border security and enhancing control of the borders between the ports of entry;
—$20 million to replace 12 of the Border Patrol's 58 Vietnam-era vintage helicopters ensuring that Agents on the ground have adequate and reliable air support;
—$5.4 million to enhance and improve the efficiency our cargo, conveyance and passenger screening systems ensuring that legitimate trade and travel crosses our borders without delay and that terrorists and their weapons, criminals or contraband are intercepted before entering the United States;
—$2.0 million for expansion of the Immigration Advisory Program to additional overseas locations ensuring that terrorists, criminals or persons traveling with fraudulent documents do not board aircraft bound for the United States;
—$5.4 million to expand the Container Security Initiative to strategically important foreign seaports;
—$8.2 million for the Customs-Trade Partnership Against Terrorism to increase supply chain security and expedite the clearance of legitimate trade;
—$1.0 million for the operating expenses associated with the Arizona Border Control Initiative;
—$3.0 million for the operation of the Automated Biometric Identification System (IDENT)/Integrated Automated Fingerprint System (IAFIS) so that CBP Officers and Border Patrol Agents can positively identify known terrorists and criminals attempting to enter the United States;
—$31.7 million to operate and maintain the long range radar system in partnership with the Department of Defense, ensuring that aircraft are detected and tracked as they attempt to enter U.S. airspace; and
—$3.2 million to contribute to the development of the DHS-wide Homeland Security Data Network.

In my statement, I will discuss these programs and others that CBP has been working on during the past year, and outline the actions CBP is planning to take in each area. I would like to begin, though, with a brief update for the Subcommittee on the status of CBP after its second year of existence as a consolidated agency within DHS.

CUSTOMS AND BORDER PROTECTION—THE SECOND YEAR

Fiscal year 2004 was the first full year that CBP operated as the single, unified border agency for the United States. From a strategic and operational standpoint, this consolidation has significantly increased our ability to execute our anti-terrorism and traditional missions at our Nation's borders more effectively than ever before, thereby enhancing the security of the United States, its citizens and the economy. I believe firmly that the United States is safer today than it was on Sep-

tember 11, 2001, because of the creation of CBP and the efforts and vigilance of CBP's personnel.

Achieve One Face at the Border

With the creation of CBP, one agency has the responsibility for the entirety of our country's borders, for all purposes, customs, immigration, agriculture protection and, importantly, terrorism. This means that for the first time in our Nation's history, we are able to design a comprehensive strategy for our borders.

To create "One Face at the Border," CBP had to unify and integrate its operations and workforce. CBP is the largest merger of people and functions taking place within the DHS. Nowhere was unification more critical than at the ports of entry (POEs) where 19,000 legacy Customs, Immigration and Agriculture inspectors joined together to carry out CBP's priority and traditional missions. To unify the Inspector workforce at the POEs, CBP established a new frontline team—the CBP officer and CBP Agriculture Specialist. In March 2004, former Agriculture Inspectors became CBP Agriculture Specialists and in July, all former Customs and Immigration Inspectors were converted to the CBP Officer position with a new series, title and job description. The two occupational groups wear the same uniform and have been unified under a single compensation system for overtime and premium pay, ensuring efficient and equitable assignment of work and compensation. This consolidation was commemorated in August when the new CBP badges with the DHS seal were issued to our personnel. Today CBP Officers and CBP Agriculture Specialists are our frontline team at all of our Nation's ports of entry and overseas pre-clearance locations.

Secure and Improve the Flow of Global Trade

For the first time ever, on December 9, 2004, the World Customs Organization (WCO) Policy Committee endorsed a Framework of Standards to secure and facilitate global trade. The WCO represents 164 Customs administrations from around the world and accounts for 99 percent of all global trade. The framework is based in large part on principles designed and implemented by CBP in the aftermath of September 11, including: the 24-Hour Rule; the Advanced Targeting System located at the National Targeting Center; the Container Security Initiative, and the Customs-Trade Partnership Against Terrorism (C–TPAT). The WCO framework encourages cooperation among worldwide Customs administrations to secure international supply chains and facilitate the movement of legitimate trade and travel.

Develop and Implement a Comprehensive Border Control Strategy

As a sovereign Nation, it has always been important that we control our borders. In light of the terrorist attacks of September 11, and the continuing threat posed to our country by international terrorists, it is now absolutely essential that we do so. and it is likewise essential that we have a coherent and understood strategy for doing so. We are developing a new Border Patrol strategy designed to achieve the goal of operational control of the United States borders. This strategy will build on the previous Border Patrol strategies, but will be enhanced to reflect the current threat environment.

CBP's Office of Border Patrol is a vital part of CBP, responsible for controlling the border between official ports of entry. In the last 2 years, the Border Patrol has made significant strides in improving our ability to control our border and establish a substantial probability of apprehending terrorists and their weapons as they attempt to illegally enter the United States between the ports of entry. For example, CBP has tripled the number of Border Patrol Agents on the Northern Border since 9/11, centralized the Border Patrol's command structure, and deployed additional technology to improve border enforcement operations, including cameras, electronic sensors, and Unmanned Aerial Vehicles.

As important as these milestones are, we cannot afford to become complacent or let down our guard. To meet the threat of global terrorism, we must implement a layered, defense in-depth strategy to protect our borders. New challenges and opportunities are on the horizon for CBP. Our achievements over the past year and the President's fiscal year 2006 budget will serve as the foundation to meet them.

Integrate Air and Marine Operations

The fiscal year 2005 Department of Homeland Security (DHS) Appropriations Act directed the transfer of missions and assets of the Air Marine Operations (AMO) from Immigration and Customs Enforcement (ICE) to CBP. The transfer will be completed in two phases. Phase One, which was completed on October 31, 2004, moved AMO intact from ICE to CBP. This included the transfer of operational responsibility and responsibility for all AMO personnel, missions, commitments, facilities, and assets to CBP.

Phase Two, which commenced in late November, is the integration of all CBP air and marine personnel, missions, and assets. To accomplish this, CBP is using the Transition Management Office (TMO) process that was used successfully during the merger of the legacy CBP entities. CBP has made significant progress in Phase Two. I am confident that upon completion of this process, we will have a more integrated, effective and efficient aviation and marine program.

Provide Assistance to the New Government of Iraq

In August, teams of CBP Officers and Border Patrol Agents were deployed to the Jordanian International Police Training Center to train officers of the Iraqi Department of Border Enforcement. The Iraqis have been provided with courses on border security tactics, human rights, defensive tactics, weapons training, and vehicle searches; in addition to basic customs and immigration activities. To date, CBP personnel have assisted in the training of more than 2,100 Iraqi border control officers. The training provided by CBP personnel will continue in the aftermath of the recent elections and focuses on keeping saboteurs, terrorists and armaments from crossing into or out of Iraq. The Iraqi officials CBP trained are now putting these skills to use at their country's borders and ports of entry.

MEETING OUR TWIN GOALS: BUILDING MORE SECURE AND MORE EFFICIENT BORDERS

As the single, unified border agency of the United States, CBP's mission is extraordinarily important to the protection of America and the American people. In the aftermath of the terrorist attacks of September 11th, CBP has developed numerous initiatives to meet our twin goals of improving security and facilitating the flow of legitimate trade and travel. The fiscal year 2006 budget will help us expand upon those initiatives to ensure further protection of both the American people and the American economy. Our strategy in implementing these initiatives involves a number of factors, including: (A) constant improvement of our targeting systems to better screen people and goods entering and departing the United States; (B) extending our zone of security outward by partnering with other countries; (C) extending our zone of security outward by partnering with the private sector; (D) deploying advanced inspection technology and equipment at our ports of entry to improve our ability to detect weapons of mass destruction; and (E) deploying advanced detection and monitoring equipment between our ports of entry to detect illegal crossings of our land borders with Mexico and Canada.

Enhancing Our Ability to Identify High-Risk People and Cargo

Information is one of the most important keys to our ability to increase security without stifling legitimate trade and travel. Good information enables us to more accurately identify—or target—what is "high risk," defined as a potential threat, and what is low risk or absolutely no risk whatsoever. The separation of high risk from no risk is critical because searching and scrutinizing 100 percent of the cargo and people that enter the United States would cripple the flow of legitimate trade and travel to the United States. What is necessary and advisable is searching 100 percent of the high-risk cargo and people that enter our country. To do this, we need to be able to identify what is high risk, and do so as early in the process as possible. CBP has several programs and initiatives that help us accomplish that task.

Automated Targeting System

The Automated Targeting System (ATS), which is used by National Targeting Center (NTC) and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to pick up anomalies and "red flags" and determine what passengers and cargo are "high risk," and therefore scrutinized at the port of entry or, in some cases, overseas.

The funding increases sought for ATS in the fiscal year 2006 budget will allow for the continued improvement of the system as well as provide it with the capacity to process the electronic data related to the ever-increasing number of people and goods entering the United States. For example, the funding will allow us to develop and implement a version of ATS that, for the first time, will be able to identify potentially high-risk travelers in passenger vehicles. It will also be used to upgrade our passenger targeting system by improving the amount of government data that the system can access and analyze as well as provide us with the capacity to train more people on the use of the system. On the cargo side, the funding will permit ATS to increase its capacity and upgrade its capabilities by utilizing cutting edge information analysis technologies developed by CBP and the private sector.

Extending our Zone of Security Outward—Partnering with Other Countries

Container Security Initiative (CSI)

To meet our priority mission of preventing terrorists and terrorist weapons from entering the United States, CBP must extend our zone of security outward—so that our borders are not the first line of defense to keep terrorists and terrorist weapons out of the United States. We have done this by partnering with other countries on our Container Security Initiative (CSI), one of the most revolutionary and successful homeland security initiatives developed and implemented after September 11, 2001.

Almost 25,000 seagoing containers arrive and are off loaded at U.S. seaports each day. That equates to nine million cargo containers annually. Because of the sheer volume of sea container traffic and the opportunities it presents for terrorists, containerized shipping is uniquely vulnerable to terrorist attack. Under CSI, which is the first program of its kind, we are partnering with foreign governments to identify and inspect high-risk cargo containers at foreign ports, before they are shipped to our seaports and pose a threat to the United States and to global trade.

The three core elements of CSI are:

—First, identifying "high-risk" containers, using ATS and the 24-hour rule, before they set sail for the United States.

—Second, performing security inspections of "high risk" containers at the foreign CSI port before they are shipped to the United States.

—Third, using technology to perform security inspections of the high-risk containers, including both radiation detection equipment and large-scale imaging machines, to detect potential terrorist weapons.

CSI continues to generate exceptional participation and support. Right now, CSI is operational in 35 foreign seaports, including: Rotterdam, the Netherlands; Le Havre and Marseilles, France; Bremerhaven and Hamburg, Germany; Antwerp and Zebrugee, Belgium; Singapore; Yokohama, Tokyo, Nagoya and Kobe Japan; Hong Kong; Gothenburg, Sweden; Felixstowe, Liverpool, Southampton, Thamesport, and Tilbury United Kingdom; Genoa, La Spezia, Naples, Gioia Tauro and Livorno Italy; Busan, Korea; Durban, South Africa; and Port Kelang and Tanjung Pelepas, Malaysia; Piraeus, Greece; Algericas, Spain; and Laem Chabang, Thailand; Halifax, Montreal and Vancouver, Canada; and most recently Shanghai, China.

I want to express my gratitude to the Committee members for their support of CSI in fiscal year 2005. With the $5.4 million increase in funding requested for fiscal year 2006, we will continue expanding CSI capabilities to ports with strategic importance or ports through which containers from high risk areas are transshipped. The fiscal year 2006 budget will allow for future expansion of the program to additional high-risk or strategic foreign ports.

Immigration Advisory Program

The Immigration Advisory Program (IAP) extends our zone of security outward by screening passengers before boarding aircraft destined for the United States. Immigration Advisory Program teams identify high risk and terrorist watchlisted passengers using the Automated Targeting System and are able to intervene by questioning high risk passengers at overseas boarding areas of foreign hub airports. They are able to check documentation of high-risk passengers prior to departure and make preliminary decisions whether the passenger will be admissible to the United States upon arrival. If potentially fraudulent identification or immigration documents are identified, or the individual's purpose poses a threat, the airline is advised not to board the passenger and the host country law enforcement is contacted. The IAP teams have access to the passenger screening information produced by CBP's NTC through the vetting of passenger manifests against terrorist watch lists and criminal databases. If a "hit" occurs or documents are found to be deficient or fraudulent, the passenger is not allowed to board the aircraft. There are two significant advantages to this approach. First, terrorists, criminals or inadmissible aliens are not allowed to board, thereby preventing their entry into the United States and/or the inconvenience and expense of an in flight diversion of the aircraft. Second, the United States Government avoids penalties and the costs of detaining the individual before being deported and the airline avoids the costs of transporting the individual back to the originating airport.

IAP is currently operating on a pilot basis in Amsterdam's Schipol Airport in the Netherlands and at Chopin Airport in Warsaw, Poland. The fiscal year 2006 budget includes $2.0 million to expand IAP to two additional overseas locations. I thank the Committee for their support of this program in the fiscal year 2005 DHS Appropriations Act.

Extending our Zone of Security—Partnering with the Trade

Customs-Trade Partnership Against Terrorism (C–TPAT)

The Customs-Trade Partnership Against Terrorism (C–TPAT) is a voluntary partnership between CBP and industry to secure international supply chains from end-to-end. C–TPAT importers secure supply chains from the foreign factory loading docks of their vendors to the port of arrival in the United States. CBP, in return, offers C–TPAT shipments expedited processing and provides C–TPAT participants with other benefits.

As C–TPAT has evolved, we have steadily added to the rigor of the program. In order to join C–TPAT, a company must conduct a self-assessment of its current supply chain security procedures using C–TPAT security criteria and best practices developed in partnership with logistics and security experts from the trade. A participant must also commit to increasing its supply chain security to meet minimal supply chain security criteria. Perhaps most importantly, participants also make a commitment to work with their business partners and customers throughout their supply chains to ensure that those businesses also increase their supply chain security. By leveraging the influence of importers and others on different participants in the supply chain, C–TPAT is able to increase security of U.S. bound goods to the point of origin (i.e., to the point of container stuffing). This reach—to the foreign loading dock—which is beyond the regulatory reach of the United States Government, is critical to the goal of increasing supply chain security.

C–TPAT is currently open to all importers, cross-border air, sea, truck, and rail carriers, brokers, freight forwarders, consolidators, non-vessel operating common carriers, and U.S. Marine and Terminal operators. We are currently enrolling certain foreign manufacturers in the C–TPAT program as well, and we will continue to develop ways to include this important element of the supply chain in the program. The intent is to increase point of origin to point of arrival security into the supply chain with active C–TPAT links at each point in the logistics process.

Although C–TPAT is a partnership, the risk is too great to simply take participants at their word when it comes to their supply chain security. We have created a cadre of specially trained supply chain security specialists to validate the commitments made by C–TPAT participants—to ensure that they are increasing supply chain security as they have promised CBP. These specialists meet with personnel from C–TPAT participants and their business partners and observe the security of their supply chains, including security at overseas loading docks and manufacturing plants, as well as transportation links outbound to the United States. Through this process, we work with C–TPAT participants to identify ways that they can further increase their supply chain security and we ensure that companies that are not honoring their commitments lose their C–TPAT benefits. As of January 12, 2005, C–TPAT had reviewed and verified the security profiles for 4,460 companies; there are more than 3,500 company profiles pending acceptance. We have validated or are in the process of validating parts of the supply chain of over 1,200 of the 4,460 certified partners, or approximately 27 percent. Our fiscal year 2006 program increase request of $8.2 million will enable outreach activities and continue validations and verifications of C–TPAT certified partner profiles.

Using Technology to Detect Weapons of Mass Destruction at our Ports of Entry

As trade increases, CBP's reliance on Non-Intrusive Inspection (NII) technology to secure the borders becomes more and more critical. Only by using NII technology to speed the inspections process for weapons of mass destruction (WMD) and contraband can CBP meet its twin goals of increasing security and at the same time facilitating trade.

CBP uses various technologies in different combinations to substantially increase the likelihood that a nuclear or radiological weapon or weapons grade material will be detected. In addition, CBP also uses NII technology to detect and interdict narcotics, currency and other contraband secreted in large containers and commercial shipments. Technologies deployed to our Nation's land, sea and air ports of entry include large-scale X-ray and gamma-imaging systems—systems that can image the contents of an entire container in minutes. These systems include the Vehicle and Cargo Inspection System (VACIS), Mobile VACIS, Truck X-ray, Mobile Truck X-ray, Rail VACIS, Mobile Sea Container Examinations Systems and the Pallet Gamma-ray System. In September 1996, our first large-scale NII system, a Truck X-ray, became operational in Otay Mesa, California. Today, we have 145 large-scale NII systems deployed.

In addition, we have developed and are implementing a comprehensive radiation detection strategy at our ports of entry. Pursuant to that Strategy, we are deploying nuclear and radiological detection equipment to include personal radiation detectors

(PRDs), radiation portal monitors (RPMs) and radiation isotope identifier devices (RIIDs). In combination with our layered detection strategy—working overseas to prevent the proliferation of nuclear materials and to detect them before they are shipped to the United States—and our use of multiple inspection technologies, these tools currently provide CBP with significant capacity to detect nuclear or radiological weapons and materials. We currently have over 400 RPMs deployed at our borders.

The fiscal year 2006 request includes $125 million to continue the acquisition, deployment, and enhancement of Weapons of Mass Destruction Detection Technology at our Nations ports of entry. These actions will be coordinated with the Domestic Nuclear Detection Office (DNDO), which is being established to develop, acquire and support the deployment of the national nuclear detection architecture, including future acquisition issues. CBP's radiation detection strategy will be integrated into the overall strategy developed by DNDO.

Our investment in WMD Detection technology is paying off as demonstrated by the following recent event. On January 26, 2005, at the Los Angeles seaport a PRD activated in proximity to a vessel from Kwan Yang, South Korea. A search of the vessel revealed that the source of the radiation was located in the ship's engine room. Subsequent screening with a Radiation Isotope Identifier and analysis by CBP Laboratory and Scientific Services Personnel stationed at the NTC revealed that the material was Cobalt 60, a material used in industrial and medical applications. Following coordination with the Science and Technology Directorate's Secondary Reachback Program, scientists were dispatched from the Department of Energy Radiation Assistance Program and it was confirmed that the radiation levels posed no threat to safety and that it was emanating from a gauge in the ship's fire extinguishing system. Although this alarm proved to be benign, the event demonstrates CBP's improving ability to detect sources of radiation in conveyances arriving at our borders and quickly take appropriate action to resolve any potential threats. Indeed, since CBP installed the first RPMs in May 2002, we have resolved over 10,000 radiation hits of vehicles or cargo shipments crossing our borders.

Detecting and Responding to Illegal Crossings Between our Ports of Entry

America's Shield Initiative (ASI)

The America's Shield Initiative, formerly known as the Integrated Surveillance Intelligence System (ISIS), is an effort to develop a comprehensive and unified system of electronic surveillance of our entire land borders. ASI is a critical part of CBP's strategy to build smarter borders. This, in turn, is critical to the Border Patrol's ability to increase its apprehension capabilities along our borders, and thereby establish greater control of our borders. The deployment of ASI is critical to prevent terrorists from entering the United States and to achieve operational control of our Nation's borders.

I thank the Committee for the $64.2 million provided for ASI in the fiscal year 2005 Appropriations Act. These resources are being used to solicit and award a contract for the nation-wide integration of legacy ISIS capabilities and to deploy additional systems along our borders. Nation-wide integrated ASI capabilities will provide the Border Patrol with a tactical, command and control, situational awareness and intelligence collection and management system. The $19.8 million requested for fiscal year 2006 would enable CBP to broaden substantially its ASI coverage of the northern and southern borders by deploying the system where no coverage currently exists. In addition, with the advent of ASI, system capabilities will be improved to enhance the sensor and video surveillance capabilities of currently installed components, integrate new, state of the market surveillance technologies and increase interoperability with other law enforcement agencies.

ASI acts as an important force-multiplier that allows CBP's Border Patrol agents to remotely monitor the border and respond to specific illegal border crossings rather than having to exhaustively patrol an area adjacent to the border. By contrast, Border Patrol operations without ASI support are not only less effective, they are more resource-intensive and less safe for Border Patrol Agents. Expanding the portion of the border covered by electronic surveillance, integration of new components and technologies, and improved Agent support equipment via the ASI program will provide the Border Patrol with the increased ability to meet its and CBP's priority mission threats.

Border Patrol Aircraft Modernization and Replacement

Aviation is one of the most effective force multipliers used in securing our Nation's borders. Aircraft perform a multitude of missions in this environment, including border surveillance, operational patrol, personnel deployment to permit rapid response to intrusions, and medical evacuation. In fiscal year 2004, CBP Border Patrol

Aircraft flew almost 46,000 hours, apprehending 96,341 persons and assisted in seizing $103.6 million in illegal narcotics. This equates to 2.1 arrests and $2,259 in seized contraband for each flight hour. The largest segment of the Border Patrol fleet is its helicopters; including 58 that are Vietnam era vintage. The high level of fight time is taking its toll on these important assets. New parts are no longer manufactured, requiring that salvaged parts be used to repair broken or damaged aircraft. The $20.0 million requested will allow CBP to begin implementation of the fleet modernization and replacement plan through the acquisition of 12 new helicopters. This initiative will improve Border Patrol Agent safety and ensure that these valuable assets, essential to effective border control, continue to be available to our frontline personnel.

Border Patrol Agent Staffing

An increase of $36.9 million is included in the fiscal year 2006 budget to enhance Border Patrol staffing by 210 Agents. The additional Agents will be deployed along the southwest border to areas with the highest concentration of illegal entry activity. To date in, fiscal year 2005, there has been a 15 percent increase in apprehensions along the southwest border when compared to the aliens from the same time period in fiscal year 2004. In addition, there has been an increase in the number of Special Interest Aliens (SIA) and High-Risk Other Than Mexican illegal entrant aliens that pose an increased threat to U.S. national security. CBP has experienced significant operational success in targeted areas. Additional Agents and supporting resources are necessary to sustain and expand the progress made in border control efforts.

Arizona Border Control Initiative-ABCI

This landmark program supporting the mission of CBP to detect and deter terrorist activities and cross-border illegal trafficking of people and drugs was initiated on March 16, 2004, in the Border Patrol's Tucson Sector. Working in partnership with Immigration and Customs Enforcement (ICE), the government of Mexico, state, local, tribal and Federal law enforcement organizations, the CBP Border Patrol-led ABCI was designed to produce a safer and more secure southwest border at one of the weakest segments of our border with Mexico.

The goals of ABCI were and are to: (1) achieve operational control of the Arizona border (2) support CBP's priority antiterrorism mission; (3) significantly impair the ability of smuggling organizations to operate; and (4) decrease the rate of violent crime and reduce the need for social services in southern Arizona. In fiscal year 2004, as part of ABCI, CBP repatriated 14,058 Mexican nationals on a voluntary basis to the interior of Mexico by means of commercial flights. This is the first successful interior repatriation effort, and it is a result of cooperation of and coordination with the Government of Mexico. These flights decreased the incidence of border crossing recidivism and reduced the number of heat related exposure deaths in the Arizona desert by 69 percent—from 45 in fiscal year 2003, to 14 in fiscal year 2004 (during the period of July 12th through September 30th). ICE will assume responsibility for the interior repatriation flights in fiscal year 2006. Our fiscal year 2006 budget request of $1.0 million will assist in offsetting the costs of CBP's continued participation in the ABCI. These resources will be used for Border Patrol Agent support costs and other operational expenses including fuel, vehicle maintenance, and overtime associated with increased border surveillance within the Arizona area of operation.

Long Range Radar

The fiscal year 2006 CBP budget includes a total of $44.2 million, an increase of $31.7 million over base resources for our share of the joint agreement with the Department of Defense (DOD) to assume financial responsibility for the operations and maintenance costs of the primary component of the Federal Aviation Administration (FAA) long-range radar system. Beginning in fiscal year 2006, CBP and DOD will share these costs equally.

Continued access to the primary component of the long-range radar system is essential to our ability protect the United States from acts of terrorism and drug smuggling via cross-border aviation. The FAA's primary radar system is used to track aircraft that either do not have transponders or have their transponders turned off in an attempt to avoid radar detection. Most small, non-commercial aircraft do not have transponders and these are the vehicle of choice for smugglers attempting to bring loads of cocaine, marijuana and heroin to the United States from Mexico and other source countries in Central and South America.

IDENT/IAFIS

The Automated Biometric Identification System/Integrated Automated Fingerprint Identification System otherwise known as IDENT/IAFIS, was established to merge the capabilities of the FBI's criminal master fingerprint file and the former Immigration and Naturalization Service's immigration violator database. These systems have been integrated into one system that captures biometric and biographical information through the use of a "10 Print" fingerprint machine and computer based facial imagery. The goals of the system are to identify repeat immigration offenders and identify criminals and previously deported aliens who should be detained. IDENT/IAFIS provides CBP's front line personnel with access to approximately 48 million criminal history records dating back to the 1920's. All Border Patrol field locations now have access to integrated IDENT/IAFIS and all CBP Ports of Entry will have access to the system by the end of this year. Previous studies indicate that combining IDENT and IAFIS checks increases the probability of identifying criminal aliens by almost 10 percent. In addition, significant efficiencies are gained by being able to electronically scan fingerprints to and get a response back from the databases within ten minutes. From October 1, 2003, through August 31, 2004, IDENT/IAFIS technology assisted Border Patrol Agents in the arrest of 138 homicide suspects; 67 kidnapping suspects; 226 sexual assault suspects 431 robbery suspects; 2,342 suspects for assaults of other types and 4,801 suspects involved with illegal drugs.

The Directorate of Border and Transportation Security has assumed ownership of the IDENT/IAFIS system. The fiscal year 2006, $3.0 million budget initiative will offset CBP's share of IDENT/IAFIS operations and maintenance costs.

AUTOMATION/INFORMATION TECHNOLOGY

Mr. Chairman, no discussion of a successful strategy to protect the American people and the American economy in the 21st century would be complete without consideration of the central importance of automation and information technology to CBP's mission.

Automated Commercial Environment

The Automated Commercial Environment (ACE) is an important project for CBP, for the business community, for our country, and for the future of global trade. If done properly, it will reform the way we do business with the trade community. It will also greatly assist CBP in the advance collection of information for targeting high-risk cargo to better address the terrorist threat. And in doing so, it will help us expedite the vast majority of low-risk trade.

The successful implementation of ACE has been and continues to be one of my top priorities as Commissioner. Increasing support from Congress and the Administration for ACE has been essential to the development of the new system. Funding of $321 million in fiscal year 2005 has enabled us to continue development and begin to expand the first installment of ACE benefits to the trade community. Indeed, since my testimony last year, I can tell you that the development of ACE and the efforts to put its capabilities to work on America's borders have continued full throttle. We have over 350 importers, brokers, and carriers using the ACE Secure Data Portal and, since June 2004, have been collecting an increasing amount of duties and fees via the ACE Period Monthly Statement. CBP is also operating a pilot test of the ACE truck cargo release software in the port of Blaine, Washington, and plans to expand this new capability to ports across our northern and southern borders. In parallel with this development, CBP is working with the DHS Chief Information Officer and the US-VISIT program to ensure compliance with the DHS Enterprise Architecture and position the ACE architecture so that it can be leveraged to support the broad homeland security mission.

Included within the $321 million for ACE is $16 million dedicated to continuing support of the International Trade Data System (ITDS). ITDS is our mechanism for coordinating intergovernmental support for ACE and ensuring that ACE meets the needs of government agencies with a need for trade data and a stake in border security. To that end, the ITDS Board of Directors has adopted a standard set of trade data as a step toward realizing the concept of using the ACE portal as the "single window" into government for the trade community. We are pleased to report that the original group of eight participating agencies in ITDS has now grown to twenty-six. Representatives from these agencies are actively involved in defining the releases of ACE software.

I want to thank Congress again for its past support of ACE. The continued support of ACE with $321 million in funding for fiscal year 2006 will enable us to keep pace with our schedule for future ACE releases including:

Account Revenue and Secure Trade Data

ACE Release 5, scheduled to be complete in fiscal year 2007 will leverage the inherent capabilities of CBP's core financial system, SAP. Release 5 will integrate the entry summary business process from manifest receipt to entry liquidation. Through this release, ACE will become the system of record for all entry summaries.

Screening and Targeting Capabilities

The Targeting Foundation scheduled for release during fiscal years 2005 and 2006 will extend ACE capabilities to entry summary processing through enhanced links to the NTC and its systems. Advanced Targeting capabilities will be expanded providing risk assessment and modeling, data mining, link analysis and pattern recognition capabilities.

Homeland Security Data Network—HSDN

The Homeland Security Data Network addresses the Department of Homeland Security's requirement for a system capable of managing and disseminating sensitive and classified information in a secure environment. The HSDN effort will streamline and modernize the classified data transmission capabilities of DHS in order to facilitate communication and collaboration within DHS and with other Federal agencies including the Department of Defense. When implemented, the HSDN will facilitate transmission of data between DHS offices and other networks including the Anti-Drug Network (ADNET), Automatic Digital Network (AUTODIN) and the Defense Message System (DMS). HSDN will provide a scalable infrastructure, capable of supporting the growth and evolution of the DHS mission. CBP's share of this DHS-wide initiative is $3.2 million in fiscal year 2006.

OTHER TRADITIONAL MISSIONS

Although CBP's priority mission is preventing terrorists and terrorist weapons from entering the United States, we know that we must—and will—accomplish that priority mission while continuing to perform our traditional missions well. Included among those missions are our responsibilities for interdicting drugs, apprehending individuals who enter the United States illegally, regulating and facilitating international trade, and protecting U.S. agricultural and economic interests from harmful pests and diseases.

Drug Interdiction

Our anti-terrorism and counter-narcotics missions are not mutually exclusive, and one does not necessarily come at the expense of the other. The initiatives we have put in place to prevent terrorists and terrorist weapons from entering the United States have enabled us to be more effective in seizing other illegal contraband, including illegal drugs. Indeed, one of the first results we saw after implementing ATS for commercial trucks on the land border was a large narcotics seizure from a targeted shipment. And, it is worth noting that the lessons we have learned in our battle against international drug trafficking will help us in the fight against international terrorism.

It would be a grave mistake for drug traffickers and other criminals to misinterpret our focus on terrorism as a weakening of resolve on other fronts. If anything, we have made life even more miserable for drug smugglers as we have intensified our overall presence along America's borders. Our heightened state of security along America's borders has strengthened, not weakened, our counternarcotics mission. As we have added staffing for both inspectors at the ports of entry and Border Patrol Agents between the ports of entry, acquired more inspection technology, conducted more questioning of travelers, and carried out more inspections of passengers and goods in response to the terrorist threat, we have seized greater amounts of narcotics. In fiscal year 2004, for example, we seized almost 2.2 million pounds of illegal drugs, and made some of the largest individual seizures ever recorded by officers safeguarding our borders.

The CBP Office of Air and Marine Operations (AMO) protects the Nation's borders and the American people from the smuggling of narcotics and other contraband with an integrated, coordinated and highly trained air and marine interdiction force. To accomplish the mission, AMO's thoroughly trained interdiction assets are deployed throughout the Western Hemisphere. The Air and Marine Operations Center (AMOC) in Riverside California, provides command, control, communications, and intelligence for those assets by assimilating information from a wide array of sensors.

Effective coordination between inspectors at the ports of entry and agents who carry out investigative activities is essential to the success of our counternarcotics

mission. For that reason, CBP will continue to cooperate closely with special agents from ICE to carry out this mission.

Apprehend Individuals Entering Illegally Between the Ports of Entry

CBP's Office of the Border Patrol is specifically responsible for patrolling thousands of miles of Mexican and Canadian international land borders. Its primary task is securing America's borders between official ports of entry by preventing the illegal entry of people, goods, and contraband across our borders.

The Border Patrol relies on agents, enforcement equipment (such as a fleet of specialized aircraft and vehicles of various types), technology (such as sensors and night vision cameras), tactical infrastructure (such as roads and vehicle barriers), and intelligence to carry out its mission. Applied in the correct combination, these resources can effectively deter, detect, monitor, and respond to illegal border crossings, as we have seen in locations such as the San Diego Sector and during operations such as Desert Safeguard.

In fiscal year 2004, the Border Patrol played a key role in safeguarding the United States from the entry of terrorists, criminals, and illegal immigrants. Among the nearly 1.2 million people apprehended by the Border Patrol in fiscal year 2004 were 643 aliens from special interest countries.

CBP will continue to work with other agencies and the Mexican Government to re-institute and increase the operational tempo of the Arizona Border Control Initiative this year. Under this initiative, CBP will aim to substantially reduce the number of illegal entries that occur in Arizona, and, as a result, will reduce the number of deaths that occur as aliens try to cross the Arizona desert. In turn, CBP will increase its ability to apprehend potential terrorists seeking to enter through the Arizona corridor.

Prevent Individuals from Entering Illegally at the Ports of Entry

With respect to preventing individuals from entering the country illegally at the ports of entry, CBP continues to stop hundreds of thousands of people a year who are inadmissible into the United States for a variety of reasons, including prior immigration violations, criminal history, or the possession of false or fraudulent documents, and potential terrorists.

We are helped in this effort by our close work with the Department of State to ensure CBP inspectors have the tools they need to verify the identity of visa holders and the authenticity of visas issued by the Department of State. Data on holders of immigrant visas is transferred electronically to ports of entry. When the electronic record is updated to reflect an immigrant's admission at a port of entry, that data is transferred electronically to the Bureau of Citizenship and Immigration Services (CIS) for production of a permanent resident card and creation of the immigrant file.

—In fiscal year 2004, CBP processed more than 262 million aliens attempting to enter the United States through the ports of entry; 643,091 were deemed inadmissible under U.S. law. CBP Officers also intercepted: 78,255 fraudulent immigration documents; recorded 1.8 million lookout intercepts; and, apprehended 399 travelers for terrorism or national security concerns. In addition, 19,740 criminal aliens attempting entry were not admitted and 566 stowaways were intercepted.

Regulate and Facilitate International Trade

CBP maintains responsibility for regulating and facilitating legitimate international trade. As I mentioned earlier, many of the initiatives CBP implements serve the twin goals of increasing security and facilitating trade. With the right level of industry partnership and the right combination of resources, we can develop innovative solutions that not only protect legitimate trade from being used by terrorists, but also create a better, faster, more productive system for moving goods and people across our borders and thus contributing to U.S. economic growth. The key to the success of this effort is partnerships, and we devote considerable time and effort to dialogue and interact with both large and small enterprises engaged in trade.

We have two major venues for engaging the trade community on an ongoing basis. The Commercial Operations Advisory Committee, created under the Federal Advisory Committee Act, is the primary group that provides advice on the CBP issues. The Committee meets quarterly and holds lively discussions on the full range of critical issues on our common agenda. The COAC was particularly important in helping us implement the Trade Act, and they most recently have worked on a series of measures to implement the Maritime Trade Security Act and to improve the Customs-Trade Partnership Against Terrorism (C–TPAT).

Another key group of our private sector partners is the Trade Support Network (TSN), whose members work on developing specific requirements for the Automated Customs Environment to ensure ACE delivers the critical functionality required by both CBP, the trade and other government agencies. The TSN recently created a Supply Chain Security Committee, which will be the focal point for helping us identify information required to achieve the end-to-end view of the supply chain and identify the parties capable of reporting that data.

As I have indicated, we have continued to work with the trade on these security and trade facilitation matters over the past year, and we will continue to do so in the year ahead. In fiscal year 2004, CBP processed 27.6 million entries of goods, a 7.9 percent increase over fiscal year 2003 levels and processed 23.5 million sea, truck and rail containers entering the United States, an increase of 5.5 percent over fiscal year 2003. CBP also collected more than $27 billion in revenue in fiscal year 2004: second only to the Internal Revenue Service in the Federal Government sector. CBP officers also completed 2,681 cargo merchandise seizures totaling almost $233 million and effected 8,586 seizures of counterfeit commodities with a fair market value of $48.4 million

To increase our effectiveness and provide national direction over trade concerns, CBP has a National Trade Strategy that focuses on priority trade issues such as revenue collection, intellectual property rights, anti-dumping and countervailing duties, textile enforcement, and risks associated with intentional or unintentional contamination of agricultural products. The goals of the National Trade Strategy are to collect the appropriate duties, protect American businesses and our economic interests from theft of intellectual property and from unfair trade practices, and from the contamination of agricultural products by aggressively targeting high-risk shipments. In addition, CBP is responsible for key deliverables in the Administration's Strategy Targeting Organized Piracy (STOP) initiative, a multi-agency effort to improve protection of intellectual property rights, such as using state of the art analytical techniques to target suspect shipments and using post-entry audits.

Protect U.S. Agricultural and Economic Interests and the Food Supply

CBP also enforces the laws and regulations pertaining to the safe importation and entry of agricultural food commodities into the United States. The traditional goals of the Agriculture Inspections (AI) program have been to reduce the risk of introduction of invasive species into the United States, protect U.S. agricultural resources, maintain the marketability of agricultural products, and facilitate the movement of law-abiding people and commodities across the borders. Accordingly, inspecting potentially high-risk travelers and cargo is critical to keeping the prohibited items out of the United States, monitoring for significant agricultural health threats, encouraging compliance with regulations, and educating the public and importers about agricultural quarantine regulations. In August, 2004, CBP Agriculture Specialists at the Port of Miami, intercepted and quarantined a shipment of habanero peppers infested with Mediterranean Fruit Fly larvae at and the False Coddling Moth. This shipment was manifested as coming from the Netherlands but was suspected of originating elsewhere. The quick actions of the CBP Agriculture Specialists prevented an incident that could have created severe economic losses to Florida's burgeoning agricultural products industry.

With the creation of CBP, the AI program has expanded its focus to include a new priority mission of preventing potential terrorist threats involving agriculture. Indeed, the threat of intentional introductions of pests or pathogens as a means of biological warfare or terrorism is an emerging concern. To address this threat and to enhance its traditional AI missions, CBP has already begun using the Automated Targeting System, and its collective expertise regarding terrorism and agriculture, to strengthen our ability to identify shipments that may pose a potential risk to our agricultural interests.

In addition, CBP working closely with the Food and Drug Administration (FDA) to implement the Bioterrorism Act to guard against threats to the food supply. The implementation of Phase III of the Act requires that prior notice of importation or intent to import all food to be consumed by humans be provided to both CBP and the FDA. Under the BTA, food products shipped by truck require two hours advance notice, by rail and air four hours and by sea eight hours. Enforcement of the provisions of the BTA are designed to protect the food that is on every table of every American household and to detect potential incidents of bio- and agroterrorism involving food. These efforts have built on our priority and traditional missions to make the food supply more secure, and will be supported in part by the targeting funding sought in the fiscal year 2006 budget.

CONCLUSION

Mr. Chairman, Members of the Subcommittee, I have outlined a broad array of initiatives today that, with your assistance, will help CBP continue to protect America from the terrorist threat while fulfilling our other important traditional missions. Because of your support, we are far safer today than we were on September 11th. But our work is not complete. With the continued support of the President, DHS, and the Congress, CBP will succeed in meeting the challenges posed by the ongoing terrorist threat and the need to facilitate ever-increasing numbers of legitimate shipments and travelers.

Thank you again for this opportunity to testify. I will be happy to answer any of your questions.

Senator COCHRAN. Thank you very much, Mr. Bonner.

Mr. Aguirre, you may proceed.

STATEMENT OF EDUARDO AGUIRRE

Mr. AGUIRRE. Thank you, Mr. Chairman. Good morning, Chairman Cochran, ranking member Byrd, and Senator Leahy. My name is Eduardo Aguirre and I am the Director of USCIS. I appear before you to discuss the President's USCIS budget request for fiscal year 2006.

PROGRESS SINCE MARCH 2003

Yesterday, as was noted, USCIS celebrated its second anniversary. Today I am looking forward to sharing with you our tremendous progress since March 2003. We are delivering on the President's promise to welcome immigrants with open arms, not endless lines. Our remarkable progress is not an anomaly, but rather a strong foundation and a new baseline from which to grow in the coming years. We secure America's promise as a Nation of immigrants by fundamentally reforming our tired system of immigration services.

FISCAL YEAR 2006 BUDGET REQUEST

USCIS is one of the largest fee-funded agencies in the Federal Government. Our 15,000 employees and contractors serve applicants throughout our broad national and international network. The President's fiscal year 2006 budget will allow us to build upon the progress we have made. The budget includes a total for USCIS of $1.854 billion, $80 million in appropriated funds and $1.774 billion in fees. This budget will allow USCIS to process over 7 million immigration benefit applications.

We note that fiscal year 2006 will be the final year of the President's 5-year plan for backlog elimination. Our budget includes a total of $100 million to support backlog elimination efforts as well as improvements in applications processing. This brings the 5-year total for this aggressive initiative to $560 million. We are on track to achieve the President's backlog elimination mandate.

As Will Rogers eloquently stated, even if you are on the right track you will get run over if you just sit there. Thus, we have taken and continue to take a hard reengineering look at the way we currently conduct our business. Since my appointment and confirmation as Director of USCIS, our leadership team has continually reviewed our processes, identified opportunities for streamlining and further improvement, and implemented meaningful changes.

Let me plainly state that as we improve our ways we are committed to never compromise national security in an effort to increase productivity. From day 1, USCIS established three crystal-clear priorities: One, eliminate the immigration benefit applications backlog; two, enhance national security; and three, improve customer service. Let me briefly touch upon progress made on each of these priorities.

BACKLOG ELIMINATION

Eliminating the backlog. Operationally, fiscal year 2004 was truly an outstanding year for USCIS and we continue the momentum so far in fiscal year 2005. We successfully reduced the backlog to 1.365 million cases, down from a high of 3.8 million cases just a year ago in 2004. We increased overall completions by 21 percent processed, met, or exceeded cycle time targets in 15 of 16 major form types. We completed 109,000 asylum cases in fiscal year 2004, a 20 percent increase, and also 53,000 refugees were admitted to the United States in fiscal year 2004, an 86 percent increase.

NATIONAL SECURITY MISSION

Ensuring national security as well as preventing and detecting fraud are essential elements of our mission. Our newly created Fraud Detection and National Security Unit developed a joint anti-fraud strategy with ICE. We enhanced our background check process and we share information with key law enforcement and intelligence agencies.

IMPROVEMENT IN CUSTOMER SERVICE

As an immigrant who once passed through the old INS system, I insist that we treat those who come before USCIS with dignity and respect. That brings me to improving customer service. Therefore, we have promoted a customer service culture and expanded many of the services available to customers online and by phone. Electronic filing now supports 50 percent of the total volume of benefit applications.

InfoPass, our web-based system, enables applicants to go online in 12 different languages to schedule appointments. No more endless lines outside our immigration offices. We expanded phone services and access to customer's case status information via our website.

Finally, in the past year USCIS has naturalized more than 7,000 military service members. This past October, I personally led a USCIS team to Afghanistan and Iraq and launched overseas naturalizations to our military.

PREPARED STATEMENT

In summary, although we have a long ways to go before our destination, I note that we are on the right track and moving forward to make USCIS an exemplary United States Government agency. This concludes my opening remarks, prepared remarks. I thank you for your support and for the invitation to testify before this subcommittee, and of course would be happy to answer your questions. Thank you, sir.

[The statement follows:]

PREPARED STATEMENT OF EDUARDO AGUIRRE, JR.

Good afternoon Chairman Cochran and Ranking Member Byrd and Members of the Subcommittee. My name is Eduardo Aguirre and I have the honor of serving as the first Director of U.S. Citizenship and Immigration Services, within the Department of Homeland Security.

We are a welcoming Nation, and the hard work and patriotism of our immigrants has made our Nation prosperous. Since USCIS was established in March of 2003, we have made tremendous progress, which I will share with you today, to deliver the President's vision of "welcoming immigrants with open arms . . . not endless lines." It is my sincere belief that the progress we have made in the past year is not an anomaly, but rather a strong foundation and a new baseline from which to grow.

USCIS will continue to secure America's promise as a Nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system. Our vision is to strengthen America's future by becoming a customer-focused innovator of benefits processing, a catalyst for citizenship education, instruction and outreach, a recognized and credible source of useful information, and a leading contributor to the security of the United States.

USCIS has established three core values: integrity, respect, and ingenuity. We shall always strive for the highest level of integrity in our dealings with our customers, our fellow employees, and the citizens of the United States. We will also demonstrate respect in all our actions to ensure that everyone we affect will be treated with dignity and courtesy regardless of the outcome of the decision. And we will also use ingenuity, resourcefulness, creativity, and sound management principles to strive for world-class results.

USCIS is one of the largest fee-funded agencies in the Federal Government—charging fees for a variety of immigration benefits from individuals seeking to enter, reside, or work in the United States. Therefore, the actual cash flow for our business operations, including a network of 250 local offices, Application Support Centers, Service Centers, Asylum Offices, National Customer Service Call (NCSC) Centers, Forms Centers, and Internet portals, varies from year to year with the number of immigration benefit applications received.

In any typical work day, our workforce of 15,000 (one-third of whom are contractors) will:

—Conduct 140,000 national security background checks.
—Receive 100,000 hits to our Internet website (www.uscis.gov).
—Answer phone inquiries from 80,000 callers at four National Customer Service Centers.
—Process 30,000 applications for an immigration benefit.
—Answer in-person inquiries from 25,000 visitors to information counters at 92 local offices.
—Issue 7,000 green cards.
—Capture 8,000 sets of fingerprints at 130 Application Support Centers.
—Welcome 3,000 new citizens.
—Welcome 3,000 new permanent residents.
—Welcome nearly 200 refugees from around the world.
—Help American parents adopt nearly 80 foreign-born orphans.
—Process the naturalization application of 50 individuals serving in the U.S. military.
—Grant asylum to 80 individuals already in the United States.

USCIS has established three priorities: (1) enhancing national security, (2) eliminating the immigration benefit application backlog, and (3) improving customer service. In our second year of operations, we have successfully reduced the backlog to 1.5 million cases (down from a high of 3.8 million cases in January 2004), expanded electronic filing to support 50 percent of the total volume of benefit applications, expanded InfoPass (a USCIS Web-based system that enables the public to go online to schedule appointments), expanded phone services to allow round-the-clock access via automated means, expanded access to customers' case status information via the USCIS website, and created the Fraud Detection and National Security Unit to work closely with the appropriate law enforcement entities in responding to concerns relating to aliens who may pose a threat to national security or public safety.

The President's fiscal year 2006 budget will allow us to build upon the progress we have made in the past year. The budget includes a total for USCIS of $1.854

billion, $80 million in appropriated funds and $1.774 billion in fees. The fiscal year 2006 budget will allow USCIS to process over 7 million immigration benefit applications and is the final year of the President's 5-year plan to achieve a 6-month cycle time standard or less for all immigration benefit applications at every USCIS office, including a total of $100 million to support backlog elimination efforts as well as improvements in application processing. This brings the 5-year total for this aggressive initiative to $560 million.

The USCIS fiscal year 2006 budget also includes two important fee-related legislative proposals. One proposal involves the removal of a statutory cap on the Temporary Protected Status processing fee. This proposal will allow the fee to be adjusted above the current $50 to recover full costs, subject to a fee review, similar to the way other immigration benefit application fees are currently set. The other proposal is a customer service enhancement that authorizes expansion of premium processing service to non-employment based applications and petitions. The Department is currently authorized to collect a $1,000 premium processing fee, in addition to the normal processing fee, for employment-based applications and petitions. This proposal would authorize the Secretary of Homeland Security to set the premium processing fee for certain non employment-based applications and petitions, such as travel documents, advance parole, employment authorization, re-entry permits, fiancé adjudications, etc., not to exceed $1,000, and in excess of $1,000 for the investor visa (EB–5) program.

Eliminating the Backlog

Although we are on track to achieve the President's backlog elimination mandate, we fully realize that funding alone will not enable us to achieve this goal. As Will Rogers so simply stated, "Even if you're on the right track, you'll get run over if you just sit there." Thus, we have taken, and continue to take, a hard look at the way we currently conduct our business. This commitment is not just one of words, but one of action. Since my appointment and confirmation as Director of USCIS, I have worked closely with the leaders in USCIS to continually review our processes, identify opportunities for streamlining and further improvement, and to implement meaningful change. Let me assure you that USCIS will never compromise national security in an effort to increase productivity.

In the past year, USCIS forwarded to the Congress a Backlog Elimination Plan that outlines the roadmap to achieve the President's mandate. We will continue to provide the Congress with quarterly progress reports on our Backlog Elimination status and achievements.

Fiscal year 2004 was truly an outstanding year for USCIS. USCIS increased overall completions by 17 percent over the fiscal year 2003 volume and met and/or exceeded cycle time targets in fifteen of sixteen major form types. In addition, USCIS completed a total of 109,000 asylum cases in fiscal year 2004, representing a 20 percent increase in productivity from the previous fiscal year, when it completed 91,000. USCIS also worked steadily with its refugee program partners to successfully meet refugee admissions levels designated by the President while ensuring that the integrity and security of the program remained intact. USCIS officers conducted refugee status interviews in 50 countries around the world and interviewed more than 70,000 refugee applicants of at least 65 different nationalities. As a result of these efforts, almost 53,000 refugees were admitted to the United States during fiscal year 2004, an 86 percent increase over the previous year's admissions.

USCIS will increase its focus on Information Technology through an enterprise-wide transformation effort to ensure that long-term backlog elimination goals are sustained, customer service is improved, fraud detection and national security capabilities are enhanced, and a technology environment is deployed to support new processes and workflow aligned with the DHS mission and the Presidential mandate for eGov standards. USCIS is currently undergoing an infrastructure upgrade of its District and Service Center operations, upgrading its web presence environment, and developing a new integrated case management system to ultimately operate in a paperless adjudication environment.

Ensuring National Security

USCIS understands that ensuring national security and preventing and detecting fraud are essential elements of its mission. As such, our newly established Fraud Detection and National Security Unit (FDNS) developed a joint anti-fraud strategy with Immigration and Customs Enforcement (ICE), hired and trained nearly 100 anti-fraud officers, and is in the midst of implementing an anti-fraud initiative throughout the United States. The FDNS is also leading the enhancement of USCIS' background check process, which is aimed at identifying applicants, beneficiaries, and petitioners who pose a threat to national security and public safety prior to

granting them immigration benefits. The FDNS is also leading USCIS' information sharing initiative with key law enforcement and intelligence agencies.

The establishment of a Refugee Corps with an expanded management support structure will provide a strong and effective overseas refugee processing program that will more efficiently identify inadmissible persons and those who are of national security interest without compromising the U.S. Refugee Program's (USRPs) humanitarian objectives. A Refugee Corps will ensure responsiveness to USRP commitments and goals, while greatly reducing the need to draw on scarce domestic program resources. It will also ensure the quality and consistency of refugee adjudications and improve the detection of refugee application fraud and the identification of security concerns relating to refugee admissions.

USCIS also implemented the Safe Third Country Agreement on Asylum with Canada to help strengthen public confidence in the integrity of the immigration system and ensure that all asylum seekers will be heard, that they will receive procedural safeguards, and that they not be removed until either Canada or the United States has made a determination on the protection claim, in accordance with national laws implementing treaty obligations.

Improving Customer Service

The Office of Citizenship continues to focus on providing information to immigrants at two key points in their journey towards citizenship: when they first become Permanent Residents and later when they are ready and eligible to begin the formal naturalization process. In the past year, the Office of Citizenship introduced an orientation guide entitled "Welcome to the United States: A Guide for New Immigrants." The guide, which will be available in 10 languages in fiscal year 2005, contains practical information to help immigrants get started in the United States, and provides information to assist immigrants in the civic integration process. The Office of Citizenship also held a series of focus groups across the United States during the spring of 2004 to hear directly from local communities about their strengths, gaps, and needs in the areas of immigrant integration and citizenship preparation. The results of these focus group discussions were published in a report called "Helping Immigrants Become New Americans: Communities Discuss the Issues."

Additionally, we have been examining the standard of knowledge in the current citizenship test to ensure that prospective and new citizens know not only the facts of our Nation's history, but also the ideals that have shaped that history. We also are working to standardize testing procedures in an effort to ensure equitable and more uniform results. Currently, a candidate in Los Angeles is, in all likelihood, not tested the same way or asked the same questions as a candidate taking the same exam on the same day in Boston.

We do not want to make the test more difficult. We do not want to make it less difficult. We want to make it more meaningful in a way that does not have an adverse impact on any particular group of applicants. Therefore, we will carefully pilot test the revised English, history, and government tests before implementing them. And we will consult with our stakeholders to solicit their input, as we have done throughout the process. Once the test development is done, the Office of Citizenship will coordinate the creation of educational materials to complement this important initiative.

Our plan is to begin implementing the new test and testing process in 2007. Given the importance of the ultimate benefit for those tested—U.S. citizenship—this process is not one that can or should be rushed. We are committed to improving the current process and to improving it in the right way.

In our commitment to modernize and enhance the delivery of immigration services, InfoPass was launched in Miami in June of 2003. InfoPass is a free, easy and convenient alternative to waiting in line. It allows USCIS customers to go on-line and use an Internet-based system to make an appointment to speak with an Immigration Information Officer at a time that is convenient for the customer. InfoPass is now available for customers at all USCIS District and sub offices.

Other conveniences available on www.uscis.gov include "E-Filing" for certain immigration applications, including the renewal and replacement of "green cards," (Form I–90). E-Filing provides a quick, easy and convenient way for customers to complete, submit, and pay fees for petitions and applications at any time, from any computer with Internet access. As a further time saver, the USCIS Web site is now set up to accept credit cards for the payment of application fees. To date, USCIS has received more than 250,000 applications through its E-Filing system. E-Filing now supports form types that account for 50 percent of the total volume of benefits applications USCIS receives annually. During fiscal year 2005, USCIS plans to combine E-Filing with the Lockbox program to further streamline our internal processes. E-Filing will also play a key supporting role in implementing Premium Proc-

essing for additional form types; the newly enacted H1–B/L–1 Visa Reform Acts; and an electronic adjudication initiative.

Additionally, the public is encouraged to use the Internet to check the status of applications filed with any of USCIS' Service Centers. Our Case Status Service Online, available in English and Spanish, allows customers who have a receipt number for an application or petition filed at a USCIS Service Center to check the status of their pending case online through the USCIS website (USCIS.gov), or by calling the toll-free telephone number of our National Customer Service Center. The Case Status Online system offers customers the option of establishing a portfolio of up to 100 cases that can be checked through a single login 24 hours a day, 7 days a week. Customers can also elect to have USCIS automatically send an email informing them of any change in status of a pending case.

In the past year, USCIS has responded to over 11,000,000 queries for verification of immigration status. USCIS provides immigration and employment authorization status information to over 126,000 government and private sector users. By providing the best possible verification services to thousands of agencies and employers, USCIS saves the Government money by ensuring that only eligible aliens receive public benefits. In addition, an employment verification pilot program authorized in 1996 and reauthorized in 2004, helps to ensure that jobs are available only to workers authorized to accept employment in the United States.

As you are aware, the National Defense Authorization Act for fiscal year 2004 authorized overseas military naturalizations. In the past year, USCIS has naturalized more than 7,000 military service members both in the United States and overseas, and posthumously naturalized 39 service members who died in service to the United States.

Finally, USCIS committed itself to the global effort to recover from the earthquake and tsunami by announcing temporary relief measures for those individuals who are unable to return to their home country due to the destruction and humanitarian crisis in Southeast Asia. USCIS is expediting the processing of certain immigration benefit applications, including requests for advance parole and relative petitions for minor children from the affected areas. USCIS also is more readily approving applications from visitors from the tsunami-affected countries who requested a change or extension of their nonimmigrant status.

This concludes my prepared remarks. I thank you for the invitation to testify before this committee and I would be happy to answer any questions.

Senator COCHRAN. Thank you, Mr. Aguirre.

ALTERNATIVES TO DETENTION

This morning National Public Radio did a report on Alternatives to Detention and the program run by the Immigration and Customs Enforcement agency using ankle bracelets to keep up with and track noncriminal aliens as they await the outcome of their immigration cases being considered and disposed of. What is the utility of this method and do you consider it more humane, more efficient, and less expensive than detaining through forcible imprisonment, or whatever other devices you have, those who you know may not be legally entitled to be in our country? Mr. Garcia?

Mr. GARCIA. Thank you, Mr. Chairman. A timely topic as there is a $5.4 million enhancement for that program in the 2006 request. We right now have eight sites where we do Alternatives to Detention and we plan to expand that two more for a total of ten.

This is a program, Mr. Chairman, that does exactly what it says. It is an alternative to detention. These are illegal aliens who would otherwise be subject to incarceration. The program is in three steps: a 30-day period with an ankle bracelet, a monitoring and reporting requirement. If the alien complies, the bracelet comes off and then it is telephonic interviews and home visits. After an additional period, it becomes only telephonic interviews.

It is extremely cost-effective, estimated at a quarter of the cost of detention space. It provides assistance to the aliens in the proc-

ess, linking them with pro bono services, et cetera. And it asks for responsibility on the part of the alien, who has voluntarily opted into this program, and that is an important point. This is a voluntary program. But it asks for responsibility on the part of the participants and if they show that, then the conditions become less onerous over time.

USE OF RADIATION MONITORS

Senator COCHRAN. Mr. Bonner, we understand too the importance of upgrading technologies in the Border Patrol area, and you highlighted that in your statement. What is the success that you anticipate from using radiation monitors? Is this a technology that has been proven? I ask this in the context with our experience in Iraq, where the weapons inspectors were using radiation monitors there and David Kay made a point of saying you can deploy these monitors, but after the sand and the heat and the other influences of nature take place you might have a useless piece of equipment there in the desert. Have you had any experiences similar to that at CBP?

Mr. BONNER. Well, first of all, the main thing that we have going in terms of detecting against a nuclear device or special nuclear materials is a combination of technology that we would deploy and we are deploying at our ports of entry principally. So there is where we have radiation portal monitors. We have completed the first two phases, which is the International Mail Facility, so every package that comes in is screened. The International Air Express Consignment Facilities are completed. We have substantially deployed well over 200 portal monitors on our northern border ports of entry with Canada. We are in the process of now deploying a significant number along our southern border ports of entry with Mexico, and we have started deployment at some of our major seaports.

We have a long way to go here. But the question is are they effective. Well, you need a combination of technology. Radiation portal monitors are highly sensitive to both gamma and neutron detection. In other words, you can have, without getting into sort of the classified area here, you can have a fair degree of confidence in the fact that you are going to detect radiation. In fact, since we started deploying the radiation portal monitors—and these are large things at our ports of entry, through every—not just commercial truck, every passenger vehicle that comes through—since we have started deploying them, we have resolved over 10,000 radiation hits.

The good news to tell you is that those radiation hits turned out to be negative. In other words, we resolved them to be naturally occurring radiation sources or radioactive material consistent with the shipment of goods. That might be, by the way, a shipment of tiles, which very frequently emits radiation that reads for thorium and so on.

So this is not the only thing, though. We combine that with our targeting system, and our NII equipment, that is our large-scale X-ray scanning machines, as well as isotope identifiers and other personal radiation detector equipment, to give us a combination of resources that improves our ability to detect against a dirty bomb coming across our border and/or potentially a nuclear device, which is obviously of the most momentous consequence one can imagine.

We have found them to be effective. Now, we are looking for—we are always looking for better technology to detect against this issue.

SIX-MONTH AVERAGE FOR PROCESSING BENEFITS APPLICATIONS

Senator COCHRAN. Mr. Aguirre, you mentioned reducing the backlog of your benefit application cases down to 1.3 million cases from a high of 3.8 million in January of 2004. I know you have devoted special funding in this area, too. Once you do not set aside dollars to bring down the backlog, are you going to be able to maintain this 6-month average of processing applications?

Mr. AGUIRRE. Senator, I am certain of that. I am certain that we are going to meet the commitment to eliminate the backlog by September 2006. In fact, I will be surprised if we do not beat that by a little. And in the process, we have re-engineered all our processes so that not only are we eliminating the backlog and perhaps put it below a cycle time of 6 months, but also making sure that we are taking care of the applications that are coming in day in and day out.

So once this 5-year commitment expires, I do not feel that we are going to need to go back to any appropriated funds for this particular endeavor.

Senator COCHRAN. We have a vote that is occurring on the floor of the Senate right now. But before we cut off the right of any Senator to ask questions, I am going to proceed and recognize Senator Byrd and Senator Leahy both if they wanted to ask questions before we go vote.

Senator BYRD. Mr. Chairman, thank you for your courtesies always.

First, let me ask unanimous consent that a letter from me to the Honorable Michael Chertoff be included in the record following my earlier statement.

Senator COCHRAN. Without objection, it is so ordered.

ANTIDUMPING/COUNTERVAILING DUTY COLLECTIONS

Senator BYRD. Thank you.

Commissioner Bonner, on December 17, 2004, Customs and Border Protection (CBP) issued its regular annual report on the Byrd Amendment trade law. The annual report describes how hundreds of millions of dollars in duties are not being collected by Customs, and the agency has been unable to explain why it cannot collect these funds.

In fiscal year 2003, the agency failed to collect $130 million in duties owed to the United States under the U.S. anti-dumping and countervailing duty laws, and CBP failed to collect an additional $260 million in fiscal year 2004. The majority of that $390 million is the result of uncollected duties on goods imported from China. The conference report accompanying the Department of Homeland Security Appropriations Act for fiscal year 2005, which was enacted in October 2004, included language that directed Customs and Border Protection to submit a report to the House and Senate Appropriations Committees by January 15, 2005, on the implementation of recommendations that were made by the U.S. Treasury Depart-

ment's Inspector General concerning the Customs and Border Protection's implementation of the Byrd Amendment trade law.

The Senate Appropriations Committee has not yet received that report. Why is this problem of noncollection growing, and what are you doing to address it? Finally, do your efforts respond to the recommendations of the Treasury Inspector General?

Mr. BONNER. Let me first of all say, Senator Byrd, that we are committed, I am personally committed, to improving our collection efforts. I am troubled that we used to say when we were settling cases that we were leaving too much money on the table here that is not collected. It is not accurate to say that we are unable to explain what the problem is. I think we have a pretty good understanding of the problems and we have taken some steps to improve our collections of antidumping and countervailing duty assessments. But let me just identify a couple of ways where we are moving forward. One of the problems in terms of collections was the insufficiency of continuous duty bonds for these kinds of high-risk shipments. These tend to be, by the way, agriculture and seafood products, a lot of it coming from China, but some other countries, and the continuous duty bonds were not nearly sufficient when the ultimate duty assessment was made by the Department of Commerce.

So we have taken steps to raise the continuous duty bonds on goods that are particularly those types of goods that are or are very likely to be subject to antidumping duties, a final order.

There were insufficient single entry bonds. In other words, we did not have recourse. So we are more diligent. We now have something that is very close to real-time monitoring of shipments that are subject to preliminary orders of commerce or potentially high-risk shipments of goods, and are raising the single entry duty bonds to higher levels that are more consistent with what we expect the ultimate duty assessment to be.

By the way, just to let you know that we have taken not just those two steps to increase the bond coverage, but we have a better mechanism now for potentially identifying circumvention of the antidumping duties. By the way, as you can imagine, there is all sorts of circumvention. It is everything from fraudulent misdescribing of the goods, so that it is not a good that was subject to an antidumping order—we have had that, by the way, with respect to catfish shipments mislabeled as groupers. I know you are interested in this issue, Mr. Chairman. But we have had that.

We have had sham companies that are set up and so forth. So we have ratcheted up our enforcement effort through our Commercial Enforcement Division and, frankly, are working very closely with ICE in nine significant and hopefully potential criminal prosecutions, but criminal investigation of fraud. We think that it would be very important to bring additional cases in this area for its deterrent value.

We are better coordinating with the Department of Commerce so that we are actually in communication with them before even a preliminary order comes out and we can take some steps.

DEFAULT OF A SURETY COMPANY

We have discussed with the Treasury Department one other issue, and that was actual default of a surety company, which was about $100 million of the total failure to collect. This was a surety company that had been approved by the Treasury Department and it defaulted on its surety bond obligations. So we are working with Treasury to make sure that the surety companies that are approved by the Treasury Department to write customs bonds are financially viable when payment time comes up.

INITIAL PRELIMINARY ORDERS IN LIQUIDATION

So we have taken all these steps. Now, there is a lag time, as you know, between the initial preliminary orders in liquidation. So it is going to take some period of time before we see substantial results here, but I do think we have taken some very important steps to identify the problem and take concrete actions that are going to improve, and I hope substantially improve, our collection rate.

Senator BYRD. Mr. Commissioner, I am heartened by your response. I know that you are very much alert to the problem. It is complex, it is difficult, and I compliment you on the way that you are working with other agencies and departments to deal with this problem. I thank you. I urge you to continue to work on it and to work even harder. I do appreciate your efforts.

Mr. BONNER. Thank you, Senator.

Senator BYRD. Mr. Chairman, let me close, because we are up against the voting situation over there. Incidentally, I have cast over 17,000 votes, but I do want to cast some today. I am going to submit the remainder of my questions, if I may, to be answered for the record.

I thank all the witnesses.

Senator COCHRAN. Thank you, Senator, for your contribution to the hearing.

ICE HIRING IN FISCAL YEAR 2006

Senator LEAHY. Just very quickly and I will put most of my questions in the record. To Assistant Secretary Garcia: When ICE was here last year it had severe budget problems, a hiring freeze. Does the fiscal year 2006 request bring ICE back to fiscal solvency? Will you be lifting the hiring freeze. If not, when?

Mr. GARCIA. Thank you, Senator Leahy. You are correct, we were here last year, we had a hiring freeze. We have taken a number of steps to address that. Working with the Department, we continue to do that. We need to take further steps. Secretary Loy testified a couple of weeks ago to that effect.

The 2006 as we have proposed it will move us forward. We will be hiring in 2006.

Senator LEAHY. All these temporary people who have been there for 3 or 4 years, does that mean they can be looking for permanent positions now?

Mr. GARCIA. That is certainly our intention, Senator. I know that there are a number of those temporary positions at our Law Enforcement Support Center up in Burlington. As we have discussed,

I only see the role of that Center expanding and becoming more important under our homeland security mission.

Senator LEAHY. Does the budget cover what you need or are you going to need reprogramming?

Mr. GARCIA. Hard to answer because, as we go along I will look at that. I have not been able to do that yet, obviously, because of the lack of clarity on some of the budget issues and the challenges we have been facing. But it is an issue that we consider a top priority.

BORDER PATROL AGENT STAFFING INCREASES

Senator LEAHY. Mr. Bonner, I mentioned before the budget only asks for 10 percent of the mandated agents. You think we need further agents on the northern border.

Mr. BONNER. Well——

Senator LEAHY. Because you are only asking for 10 percent of what Congress mandated.

Mr. BONNER. As you know, Senator, I am in full, violent support of the President's budget request, which requests 210 Border Patrol agents in addition to, of course, replacing attrition.

Senator LEAHY. But none of them for the northern border?

Mr. BONNER. Well, you know, you did note——

Senator LEAHY. We needed more.

Mr. BONNER. You did note and let me note that we had 360 Border Patrol agents on the northern border for the entire border with Canada on 9/11. On March 1, 2003, that was up to about 500.

One of the first actions I took was to direct Border Patrol to meet the 1,000 goal, which they did actually in fiscal year 2003.

Senator LEAHY. Do we need any more—this is what the bottom line is. Do we need any more on the northern border? Do we have enough on the northern border today?

Mr. BONNER. You mean beyond what we have in the request?

Senator LEAHY. No, no. Do we have enough on the northern border with the number we have today. There is no request for the northern border. It is 210, 10 percent of what we mandated. But that is not for the northern border.

Do we have enough on the northern border? It is an easy answer, yes or no.

Mr. BONNER. We do not have enough agents. We do not have enough technology to give us the kind of security we need on the northern border.

Senator LEAHY. I am just a lawyer from a small town in Vermont. I do not understand. Is that a yes or a no?

Mr. BONNER. I am just a lawyer from a small town in Kansas, so—

That moved to California at some point.

Senator LEAHY. Here we are in the big city. Is it yes or no?

Mr. BONNER. Well, we need more agents——

Senator LEAHY. Help me out here.

Mr. BONNER. We need more agents. But look, I think it is the right combination of people and technology, and essential to this is the American Shield Initiative. The fiscal year 2006 budget includes $81 million for technology, for more helicopters, and for UAV's for the Border Patrol. We need to do a smarter and a better

job. I think we can do that. The President's request is for 210 more Agents. I do not know that they are necessarily earmarked all for the southern border. If you are asking me, I think probably most of them will go there.

Senator LEAHY. We should have this discussion in greater detail, because I am not happy. I do not think we are getting the number, we are certainly not getting anywhere near the number that the Congress mandated.

I–91 CHECKPOINT

I also want to have your staff and mine talk about this checkpoint you have on Interstate 91 in Vermont, a long, long distance from the border, that just stops honest Vermonters that have been driving back and forth there forever and ever.

You had people—aliens that have been there for ever and ever, they keep getting stopped over and over and over again. There is a real suspicion of some racial profiling people who have honestly, working in New Hampshire and Vermont for years and years, and just continuously get stopped. They continuously get asked the same questions as they got asked the day before.

The irony is, of course, if anybody wanted to circumvent that they would just go out one of the back roads, and the agents would never find them.

So let our staff talk about that. It is creating, both in the "Live Free Or Die" State of New Hampshire and the former independent republic of Vermont, it is creating a bit of a concern. It is not going to do anything to stop people from coming across the border, because they are not the ones getting stopped.

Mr. BONNER. Could I briefly respond, though? That is that part of the strategy is not putting everything on the line itself. There has to be a second line of defense. It is not that the checkpoint is necessarily going to—that terrorists that might come across the Canadian border into the United States. Part of the strategy of a checkpoint is lateral enforcement from the checkpoint. It gives us a second line of defense.

Senator COCHRAN. Senator, we have a vote.

Mr. BONNER. It is going to be important. It is an important part of the overall strategy to get better control of our borders, something you and I have a common interest in.

Senator LEAHY. Yes. But when I have to stop and prove my identification and I am a U.S. citizen, I know this is helping somebody. It is sort of like security stopping Ted Kennedy a dozen times from going on a plane because he is seen on a terrorist list and the government does not know how the hell to get him off it.

Thank you.

Mr. BONNER. Thank you, Senator.

Senator COCHRAN. This Senate hearing will stand in recess until we go vote and we will return to resume our questioning of the witnesses. We appreciate your indulgence.

NEW OFFICE OF SCREENING COORDINATION AND OPERATIONS

Thank you very much for your patience. I apologize for having to go vote on the floor of the Senate during our hearing.

The President's budget proposes to create the Office of Screening Coordination and Operations within the Border and Transportation Security Directorate. How do each of you see this new office contributing to the Department's ability to implement the 9/11 Commission recommendation? Mr. Bonner, let us start with you.

Mr. BONNER. Well, I would say this, that certainly there will be some benefits from thinking through this issue of screening, particularly for the terrorist threat. So I expect that it will assist in terms of coordinating those efforts, understanding that there are fundamentally very different screening opportunities that are presented depending upon which homeland security agency you are talking about.

We have the broadest law enforcement authority of any law enforcement agency in our country, Customs and Border Protection, and that is because we have the full authority to, without cause or suspicion, ask questions of anybody who is crossing our border or entering our country through our official entry points and certainly to arrest anybody who is not. Secondly, we have the broad customs search authority, which is the broadest search authority under the Fourth Amendment of our Constitution, which permits us to search and inspect luggage of everybody, by the way, U.S. citizens, noncitizens, without cause, warrant, or suspicion.

So we have broad authorities, which we are using right now in terms of being as intelligent as we can to perform that priority mission of preventing terrorists from entering our country. But I think nonetheless the Screening Coordination Office should, I believe, play a helpful role.

VETTED TRAVELER PROGRAMS

There is another area, just briefly let me touch on it, Mr. Chairman, where the Screening Coordination Office I think could play a valuable role. That is, there are in place right now essentially what I call trusted, vetted traveler programs. Customs and Border Protection vastly expanded the Nexus program at the Canadian border. We now have almost 80,000 people that we have vetted. That is not only taking biometrics from them; that is a personal interview to make sure that they pose no terrorist threat or smuggling threat. We have a similar program that we inherited from INS, the SENTRI program at the Mexican border. We have FAST, the FAST program for commercial truckers from both Mexico, coming from Mexico or Canada, and so forth.

We have mature actual programs. They are not pilots. We have enrolled about 200,000 people into these programs. But on the other hand, TSA is piloting a registered passenger program and so forth. You need to look at the issue of what are the biometrics that should be collected from each person that is enrolled or is going to be considered to be a trusted or registered individual for receiving some benefits. You need to look at the biometric you use to identify them when they appear at the border port of entry or when they appear at the airport if it is a TSA issue and the like, and so forth.

I think the Screening Coordination Office could play a very important role in getting those policy decisions, and they are policy decisions, made and implemented in the most visionary way possible, so that at the end of the day somebody that is vetted in for

one of these programs, let us say for the Nexus program, would be cleared in for other kinds of trusted passenger programs.

That is a big idea and I think the Screening Coordination Office can and I hope will play a valuable role in harmonizing, if you will, the technology issues for these different kinds of trusted, vetted, or registered passenger or traveler programs.

Senator COCHRAN. Mr. Garcia, this was part of the presidential commission, the National Commission on Terrorist attacks, the 9/11 Commission's, recommendations, that there be a centralized office created, designed to provide comprehensive screening across, addressing common problems and setting common standards in a systemwide operation. Do you see this office contributing to the Department's ability to implement this recommendation?

Mr. GARCIA. Thank you, Mr. Chairman. Yes, absolutely. Again, you tie it back to the 9/11 Commission report. I think you also look at the staff report on terrorist travel, the recommendations in there, incredibly important work, the conclusion that terrorist travel is at least as important an area or vulnerability as terrorist financing. This center certainly moves us forward in addressing those vulnerabilities. ICE will play a role, as we will CBP and CIS, in working with that center. For example, as we discussed, people who are screened who are turned back we now can follow through with associates present in the country by looking at our systems and our data.

We can use our forensic document lab to examine their travel documents and provide bulletins and intelligence analysis to the front-line folks by analyzing that travel documentation that terrorists or other national security threats use to try to enter the country.

So certainly centralization of the screening function, and as importantly I think what will flow from that within the Department and within the agencies.

Senator COCHRAN. Mr. Aguirre, does this affect your agency and how are you cooperating in this effort if so?

Mr. AGUIRRE. Mr. Chairman, it does affect our agency because, of course, we are all in the immigration business to one extent or another. Even though we are not on the enforcement side, we are involved in the biometric of, capturing biometrics of millions of applicants year in and year out, and those biometrics of course are oftentimes being used for law enforcement purposes where necessary.

I actually view the issue from a service standpoint, in contrast to the enforcement standpoint. Any time you can have consistency and coordination of the identification process and the biometrics and so on, it can be an expedited opportunity for those who do not have hits or do not have any reason to feel the need of scrutiny.

So I think it would expedite the processing of the 97, 98 percent of those individuals that cross in and out. As you probably know, USCIS is the organization that generates many of the cards that are being used today. For instance, the Green Cards are produced by us. We have put in those Green Cards—permanent residency card—any number of biometric data for our colleagues on the enforcement side to be able to work with.

OFFICE OF SCREENING COORDINATION AND OPERATIONS MISSION

Senator COCHRAN. Commissioner Bonner, should the Office of Screening Coordination and Operations have actual operational authority for various screening programs, as proposed, or should it focus on the integration and coordination function necessary across so many programs involved in the activity?

Mr. BONNER. I would say with respect to operations, you are talking about the actual gathering of biometric data on potential enrollees. You are talking about the actual interview that we do and have done with a couple hundred thousand people. I think that probably should be an operational function left with the agency that is ultimately responsible for and going to be held accountable for whatever benefit is being given.

If you took just the border issue in terms of our screening at our ports of entry, international airports, land border, ultimately CBP is operating these programs right now—the NEXUS program, the SENTRI program. It may well make sense to leave that operation at the agency level, in the agency that actually is responsible.

Now, having said that, let me say we have a new Secretary of Homeland Security, Mike Chertoff. By the way, I think Secretary Chertoff is somebody who, based upon my past experience, is going to be an extraordinary Secretary. He ultimately makes the decision, not me, as to how you make this distinction between what operational functions should remain at the agency level and what, if any, systems functions should be performed by the Screening Coordination Office.

I do not think that has been decided. Those are my views subject to, of course, further guidance from Secretary Chertoff.

Senator COCHRAN. Director Aguirre, what is your take on that? Just from an opposite point of view, should the Citizenship and Immigration Services programs, screening programs, be moved to the Office of Screening Coordination and Operations?

Mr. AGUIRRE. Mr. Chairman, I am not sure that in the vacuum of this hearing I can give you an accurate answer. I think the issue of operations and the issue of "who is responsible for what" needs to be weighed in the context of is it working well/is it not working well/and how can it work better. So within Homeland Security I think we have a number of components that can always stand improvement, and to determine here and now what is better or worse, I would be ad libbing.

INTELLIGENCE REFORM ACT/BORDER PATROL STAFF INCREASES

Senator COCHRAN. Mr. Bonner, this request does not include resources to fulfill the new Intelligence Reform and Terrorism Prevention Act authorizations. Were the new authorizations considered or was the bill enacted into law too late to be considered when the fiscal year 2006 budget process was completed inside the administration?

Mr. BONNER. That is a good question. I need to probe my memory on it in terms of the time line. Obviously, as you know, the process is that we did make a request that goes through the Department process, and ultimately ends up getting a lot of scrubbing and review. I actually participated in the Departmental Resources

Review Board. I am not on that Board, but I was allowed to be present and to present the CBP budget request.

I need to get back to you. I do not have the time line clearly in mind, but I do not remember as I was presenting the CBP budget to the Department that the intelligence bill I do not believe had passed with that authorization level. In fact, I am just reminded it was not signed until December 17, 2004. So it may have been one of those things where the budget was being put together before we even knew what the Congressional intent was in the intelligence bill.

That said, by the way, let me say that—and I was addressing this a little bit with Senator Leahy—we have in the last 10 years or so, literally tripled the size of the Border Patrol, from about 4,000 Border Patrol Agents in the mid-90's to now, and with the President's request it will be just about 11,000 Border Patrol Agents.

There is a limit, by the way, in thinking of bringing new agent resources on board, there is a limit to how much a law enforcement organization like the Border Patrol can absorb. There are limits to how many agents the Border Control can recruit, hire, and train in a single year, and still maintain its cohesiveness as a law enforcement organization.

But that is going beyond your question, Senator. I think the answer is I do not believe that the 2000 number was out there as the budget request was going forward.

IMPLEMENTATION OF THE VISA REFORM ACT

Senator COCHRAN. Mr. Aguirre, the Visa Reform Act was passed as part of the fiscal year 2005 Consolidated Appropriations Act. That act tightens controls on the L1 visa and expands the cap on the H1B visas. What steps have been taken to begin implementation of that act?

Mr. AGUIRRE. Well, Mr. Chairman, on the L1B visas there is a provision for additional resources, human resources, to be ensured that we can prevent fraudulent applications on the L1B. I think you are clearly aware that fraud is a major issue for Immigration Services, and L1B visas in particular are ones that we have felt, and I think the Congress has felt as well, that it is vulnerable to fraud. Therefore we are putting additional human resources and applying our fraud detection and national security unit to make sure that the applications are properly processed, and expedited in the normal process, but that we identify if there are any indices of fraud that we can identify appropriately.

L1 VISA INTER-AGENCY TASK FORCE

Now, on the H1B applications, as you know, there is a provision for an additional 20,000 applications, or the cap is raised by 20,000. We are in the process of implementing that number and within the next few days, if not weeks, we will have an improved process to take advantage of that.

Senator COCHRAN. Has the L1 Visa Inter-Agency Task Force been set up?

Mr. AGUIRRE. Senator, I am not aware of that, no, sir.

UNFAIR TRADE PRACTICES—CATFISH IMPORTS

Senator COCHRAN. Mr. Bonner, this committee is interested in the progress to protect American industries from unfair competition. You mentioned the catfish and grouper issue a while ago. Of importance of course in our State and in the South is the catfish industry and the enforcement of antidumping orders in connection with Vietnamese tra and basa. What are ICE and CBP doing now to enforce this antidumping order?

Mr. BONNER. Well, I can tell you, Senator, that going back to October of last year we began a special enforcement effort to essentially identify the misdescription, mislabeling of catfish, imported catfish that would be subject to antidumping duties. We do have a laboratory science and services branch where we were taking samples literally of imports that were coming into the port of L.A., Long Beach, Miami, and the Port of New York, and determining whether in fact they were what they were represented to be. We found that there was significant misdescription of a product that was being shipped from Vietnam.

We have taken three important actions. One, based upon that identification at the port levels, we have raised the continuous duty bonds. We are requiring higher single entry duty bonds with respect to product that we believe in fact was subject to the countervailing duties, that is to say was in fact catfish. We have required payment of additional duties. We are actively pursuing what are called section 1592 penalty actions against those importers who imported mislabeled, I might say falsely and potentially fraudulently mislabeled product. We are working with ICE, as I indicated to Senator Byrd, to attempt to get further investigation through the ICE special agents, and potentially we are hopeful to get criminal prosecutions in at least some of these cases in conjunction with the Department of Justice and the relevant U.S. attorney's offices.

Clearly, we have taken some steps. We are moving out on this issue because there is clearly some false labeling that is taking place here to essentially circumvent and fraudulently evade the antidumping duties.

Senator COCHRAN. Mr. Garcia, you have some responsibilities in this area as well, do you not?

Mr. GARCIA. Yes, I do, Mr. Chairman. ICE, as Commissioner Bonner indicated, is responsible for investigations in this area. We are committed to doing that. I know this crime has a very real impact on industries in this country. I have spoken with a number of members of Congress about those impacts in their particular districts and particular industries.

I have seen a number of significant cases, and again Commissioner Bonner touched on them, that have come across my desk. I believe that we will be moving forward, again with the relevant U.S. attorney's office, to seek to bring criminal charges in a number of cases. We are using our overseas assets very aggressively to root out some of the fraud that has been going on in this area.

So we have made progress and we are committed to continuing those enforcement efforts.

BORDER PATROL AIRCRAFT REPLACEMENT

Senator COCHRAN. Mr. Bonner, the budget request includes some money, $20 million, to begin replacing Border Patrol helicopters. The plan calls for the full replacement of the air fleet to be completed in 2010. Is the request that is included in the budget sufficient to get you started in this direction? Would additional resources allow you to speed up the replacement of the fleet?

Mr. BONNER. I am happy to get started on the recapitalization of the Border Patrol air assets. As I think you know, Mr. Chairman, out of the 110 or so air platforms that the Border Patrol has, roughly—this is a rough estimate as I do not have the exact number, about 40 to 50 of those are Vietnam vintage aircraft—the OH–6's, the small bubble surveillance helicopters, as well as about maybe 10 or 12 Vietnam vintage Hueys.

It is a good start. As we move forward with the integration of the Air and Marine Office in a better configuration with the Border Patrol air assets, we are going to find that there are some benefits there in terms of how we look at the air resources we need.

But nonetheless, there is a significant amount of recapitalization that is going to need to be done and this is a start on it. Yes, Mr. Chairman, if there were more funding it would help us get there faster.

INTEGRATION OF CBP AIR AND MARINE ASSETS

Senator COCHRAN. The integration of the air and marine resources has begun, as you point out. What progress is being made toward integrating the units with the Border Patrol?

Mr. BONNER. There is some good progress. First of all, of course, the first phase of it was essentially the integration or the transfer. In some ways I see it as a transfer back to U.S. Customs, but anyway it was the transfer in November of last year of the Air and Marine Operations (AMO) office to CBP. That was phase one. That has been completed.

We are now into phase two. In phase two, I am using the Transition Management Office process that we used very successfully to unify and integrate CBP. It is a process that essentially looks at the ways that we can now further integrate essentially the air assets and also the marine assets that are now all within CBP.

By the way, there have already been some very important benefits from this, from the transfer of AMO to CBP in terms of better operational coordination between the Border Patrol and AMO and the like. But phase two will do this. It will better integrate one procurement, for not just the Border Patrol and not just for AMO, but for both. It will better integrate one maintenance system for all aviation air assets, one training system for all of our pilots, whether they are from the Border Patrol or whether they were AMO pilots. Ultimately, as part of this process, we are going to determine ways to better operationally integrate the efforts of both of these air and marine groups and assets.

I have had several briefings on this already. I believe that we will be able to make some key decisions along the lines I have described certainly in the next couple of months or so, so that we are continuing to move forward with the best optimal organization, if

you will, of the sum total of the air and marine assets that are now within CBP.

Senator COCHRAN. I appreciate very much the cooperation of each of you and your agencies with our committee and the requests that we submit for information from time to time. Particularly, I appreciate your taking time to come here today and participate in this hearing, which is very important for us to have to get a full understanding of how you are allocating the resources under the budget request and what the priorities are.

ADDITIONAL COMMITTEE QUESTIONS

We want to help you succeed in your activities. So we thank you very much for your cooperation with our subcommittee. Senators may submit questions to you in writing and we ask you to respond to those within a reasonable time for our committee record.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing:]

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

CONTINUED FUNDING SHORTFALLS—ICE

Question. In September of 2004, this Committee approved a request to transfer and reprogram $152 million in order to allow Immigration and Customs Enforcement (ICE) "to effectively manage its financial position through year end". In other words, the request was to move $152 million to ensure that ICE did not have a shortfall.

This Committee worked with the Department to permanently move $193 million in base resources from Customs and Border Protection to ICE in the fiscal year 2005 Appropriations Act. Admiral Loy recently testified to the House Appropriations Committee that he expects there to be a reprogramming request submitted soon to provide anywhere from an additional $250 to $300 million to ICE in order to finish out fiscal year 2005.

The cycle of stopgap solutions needs to end. Too much time seems to have been spent trying to figure out how this situation came about—what is termed "mapping"—rather than trying to make sure this problem is resolved so that we can move forward to ensure that an agency vital to combating terrorism is solvent.

When will this Committee receive the transfer/reprogramming proposal to address the fiscal year 2005 shortfall?

Answer. The notification of the proposed reprogramming was transmitted to the Appropriations Committees on March 12, 2005, in a letter dated March 11, 2005.

Question. Have Congressional initiatives funded in the fiscal year 2005 Appropriations Act been deferred until this problem is resolved?

Answer. In the proposed reprogramming, ICE is proposing to defer $85.216 million of the $193.916 million in enhancements, i.e., Congressional initiatives, funded in the fiscal year 2005 Appropriations Act. Item 2, on page 5 of the Report of Proposed Reprogramming Action discusses, in detail, the enhancements which are being reduced from their original appropriated amounts. The enhancements that have been reduced are shown below:

Fugitive Operations

The enhancement is reduced to $9 million from the appropriated $50 million level. This will allow funding of 42 positions instead of the 236 positions originally planned. The reduction will mean that fewer Fugitive Operations teams can be deployed as originally planned.

Institutional Removal Program

The enhancement is reduced to $4 million from the appropriated $30 million level. This will allow funding of 37 positions instead of the 279 positions originally planned. Higher cost Special Agents will continue to perform some institutional removal duties, instead of replacing all of them with Immigration Enforcement Agents.

Compliance Enforcement Units

The enhancement is reduced to $11 million from the appropriated level of $16 million. This will permit funding of 89 positions instead of the 130 positions originally planned.

Alternatives to Detention

The enhancement is reduced to $2 million from the appropriated level of $11 million. This will permit funding of 11 positions instead of the 60 positions originally planned. Some capacity increases will occur at each of the current eight Intensive Supervision sites, though not to the anticipated levels.

Guantanamo Migrant Operations Center

The enhancement is reduced to $2 million from the appropriated level of $6.2 million. The level should be sufficient to support the Center's operations. (Note: remaining, fully-funded, enhancements include $26.5 million for Detention Bed Space; $25 million for Benefit Fraud; $14 million for the Visa Security Unit and the Office of International Affairs; $6 million for the Immigration Court Backlog; $5 million for Worksite Enforcement; and, $4.2 million for the Cyber Crime Center.)

Question. What assurance do we have that the fiscal year 2006 request for ICE will solve this problem permanently?

Answer. The full funding level requested in the President's Budget, internally realigned for the impact of the fiscal year 2005 reprogramming request, will allow ICE to carry out its mission during fiscal year 2006. We do not foresee the need for further reprogramming or funding transfers among bureaus.

Question. ICE has now lived under a hiring freeze for close to a calendar year. What impact is this having on the organization's ability to carry out its mission?

Answer. ICE has had to implement several measures to ensure it operates within existing resources. It has had to prioritize funding requirements. In all cases, ICE has worked to ensure that mission critical requirements have been funded with the intent of minimizing any adverse impact on its national security related mission.

Question. There are significant resources requested for fiscal year 2006 to increase the base funding available to ICE: $105 million for the Office of Investigations, $24 million for the Office of Detention and Removals, and a significant portion of the $90 million for Custody Management. What method was used to come up with these estimates?

Answer. Estimates were derived by looking at the entire operation and determining that the resources of these offices/programs needed increases in order to attain key operational goals.

Question. Will the fiscal year 2006 request provide ICE with the funding necessary to enable it to lift the hiring freeze on October 1, 2005?

Answer. ICE continues to work closely with DHS, BTS, and OMB to identify solutions to address its financial issues. One of ICE's priorities is to implement financial solutions that will allow the lifting of the hiring freeze. This work is ongoing and as a result, it is too early to state whether the hiring freeze will be lifted on October 1, 2005. An alternative may be to implement solutions that would allow the freeze to be lifted later in the fiscal year.

Question. According to the just delivered "ICE Financial Management Overhaul" report, "The ICE Assistant Secretary brought in a team from other components of DHS on a 90-day detail to help identify solutions to ICE's financial issues. The team will make recommendations to the Assistant Secretary by later this Spring." Its charter includes: development of short-term recommendations to address fiscal year 2005 funding issues; an action plan with key recommendations to place ICE into a stable funding position for fiscal year 2006 and beyond; and recommendations for policies and procedures that will result in transparent budget and financial planning and execution. What potential is there that these recommendations could cause significant revisions to the President's fiscal year 2006 budget request?

Answer. The President's Budget includes the necessary funding to ensure ICE can accomplish its mission to detect vulnerabilities and prevent violations that threaten national security. As mentioned in the "ICE Financial Management Overhaul" report, the team is developing recommendations to improve ICE's financial position in 2006.

As noted in your question, the final report is due to the Assistant Secretary later this spring. The team's recommendations will be shared with the ICE's new CFO and Budget Director. ICE appreciates your interest in this effort and looks forward to working with you and your staff where necessary to implement any recommendations.

Question. How is it that this organization is almost 2 years old and is just now looking to develop sound financial planning policies and procedures?

Answer. The creation of the Department of Homeland Security represented a reorganization unprecedented in the Federal Government. 2005 represents the first year that ICE has focused on issues other than transition and reconciliation. It is an opportune time to further refine financial policies and procedures previously implemented and to continue developing sound policies and processes as necessary.

Question. ICE has two outsourcing competitions on going—labor management and intelligence support. Is this an area where ICE could see significant cost savings?

Answer. Fiscal year 2005 would have been U.S. Immigration and Custom Enforcement's (ICE's) initial full year of participation in competitive sourcing since its inception. ICE intended to initiate its original studies on a relatively small scale in order to properly establish its competitive sourcing infrastructure. Significant cost savings were not expected to be realized based on the fiscal year 2005 studies. More significant savings would be anticipated based on broader studies under consideration for fiscal year 2006. ICE expects to be an active participant in the initiative in fiscal year 2006.

Question. Please provide a chart with the on-board staffing level for ICE, by position type, for September 30, 2004, and fiscal year 2005 through January 31, 2005, both excluding Air and Marine Operations.

Answer. Attached are the ICE on-board staffing charts for the end of fiscal year 2004 and fiscal year 2005, through the pay period ending February 5, 2005. Federal Protective Service positions are included, but Federal Air Marshal Service positions are not included.

Highlighted changes from 2004 to 2005 are:

—An increase of 185 positions transferred from Customs and Border Protection to ICE for International Affairs

—The movement of 112 Organized Crime Drug Enforcement Task Force positions from reimbursable to direct

—The movement of 138 positions from reimbursable to direct

ICE On-board Staffing Level for the end of FY 2004	FULL TIME PERM	OTHER THAN PERM	TOTAL	TOTAL REIM	TOTAL
GS-00xx, Miscellaneous Occupations Group	1,034	6	1,040	0	1,040
GS-01xx, Social Science, Psychology, and Welfare Group	476	1	477	7	484
GS-02xx, Human Resources Management Group	52	4	56	0	56
GS-03xx, General Administrative, Clerical, and Office Services G	1,193	163	1,356	31	1,387
GS-04xx, Biological Sciences Group	0	0	0	0	0
GS-05xx, Accounting and Budget Group	255	14	269	0	269
GS-06xx, Medical, Hospital, Dental, and Public Health Group	2	0	2	0	2
GS-07xx, Veterinary Medical Science Group	0	0	0	0	0
GS-08xx, Engineering and Architecture Group	18		18	1	19
GS-0905, General Attorney Series	567	42	609	0	609
GS-0950, Paralegal Specialist Series	23	0	23	0	23
GS-0962, Contact Representative Series	0	0	0	0	0
All other GS-09xx, Legal and Kindred Group	143	6	149	0	149
GS-10xx, Information and Arts Group	49	57	106	0	106
GS-11xx, Business and Industry Group	100	3	103	0	103
GS-12xx, Copyright, Patent, and Trademark Group	0	0	0	0	0
GS-13xx, Physical Sciences Group	22	0	22	0	22
GS-14xx, Library and Archives Group	2	0	2	0	2
GS-15xx, Mathematics and Statistics Group	0	0	0	0	0
GS-16xx, Equipment, Facilities, and Services Group	19	0	19	4	23
GS-17xx, Education Group	25	6	31	0	31
GS-1801, Detention and Deportation Officer	903	2	905	0	905
GS-1801, Immigration Enforcement Agent	2,103	10	2,113	0	2,113
GS-1801, Air and Marine	0	0	0	0	0
All other GS-1801	223	0	223	17	240
GS-1802, Detention Enforcement Officer (1802)	27	21	48	0	48
All other GS-1802	1,000	133	1,133	10	1,143
GS-1811, Criminal Investigator	5,391	0	5,391	638	6,029
GS-1884 Patrol Officer	0	0	0	0	0
All other GS-18xx, Investigation Group	1	16	17	17	34
GS-19xx, Quality Assurance, Inspection, and Grading Group	7	0	7	0	7
GS-20xx, Supply Group	24	1	25	0	25
GS-2181, Pilots (2181)	0	0	0	0	0
All other GS-21xx, Transportation Group	21	0	21	0	21
GS-22xx, Information Technology Group	174	0	174	0	174
WG	120	4	124	0	124
Other (Non-WG)	0	0	0	0	0
TOTAL	13,974	489	14,463	725	15,188

Data Excludes Air and Marine

ICE On-board Staffing Level for Pay Period Ending February 5, 2005	FULL TIME PERM	OTHER THAN PERM	TOTAL	TOTAL REIM	TOTAL
GS-00xx, Miscellaneous Occupations Group	1032	2	1034	0	1034
GS-01xx, Social Science, Psychology, and Welfare Group	474	2	476	7	483
GS-02xx, Human Resources Management Group	48	3	51	0	51
GS-03xx, General Administrative, Clerical, and Office Services Group	1180	148	1328	24	1352
GS-04xx, Biological Sciences Group	0	0	0	0	0
GS-05xx, Accounting and Budget Group	249	15	264	0	264
GS-06xx, Medical, Hospital, Dental, and Public Health Group	2	0	2	0	2
GS-07xx, Veterinary Medical Science Group	0	0	0	0	0
GS-08xx, Engineering and Architecture Group	18	0	18	1	19
GS-0905, General Attorney Series	565	42	607	0	607
GS-0950, Paralegal Specialist Series	23	0	23	0	23
GS-0962, Contact Representative Series	0	0	0	0	0
All other GS-09xx, Legal and Kindred Group	133	4	137	0	137
GS-10xx, Information and Arts Group	45	54	99	0	99
GS-11xx, Business and Industry Group	94	2	96	0	96
GS-12xx, Copyright, Patent, and Trademark Group	0	0	0	0	0
GS-13xx, Physical Sciences Group	21	0	21	0	21
GS-14xx, Library and Archives Group	1	0	1	0	1
GS-15xx, Mathematics and Statistics Group	0	0	0	0	0
GS-16xx, Equipment, Facilities, and Services Group	19	0	19	4	23
GS-17xx, Education Group	24	5	29	0	29
GS-1801, Detention and Deportation Officer	896	2	898	0	898
GS-1801, Immigration Enforcement Agent	2122	14	2136	0	2136
GS-1801, Air and Marine	0	0	0	0	0
All other GS-1801	193	0	193	16	209
GS-1802, Detention Enforcement Officer (1802)	5	18	23	0	23
All other GS-1802	981	115	1096	3	1099
GS-1811, Criminal Investigator	5619	0	5619	383	6002
GS-1884 Patrol Officer	0	0	0	0	0
All other GS-18xx, Investigation Group	2	20	22	0	22
GS-19xx, Quality Assurance, Inspection, and Grading Group	8	0	8	0	8
GS-20xx, Supply Group	23	1	24	0	24
GS-2181, Pilots (2181)	0	0	0	0	0
All other GS-21xx, Transportation Group	20	0	20	0	20
GS-22xx, Information Technology Group	178	1	179	0	179
WG	119	4	123	0	123
Other (Non-WG)	0	0	0	0	0
TOTAL	14094	452	14546	438	14984

Data excludes Air and Marine

Question. Please provide updated fee projection charts for each fee account for fiscal year 2006 as compared to fiscal year 2005, with the chart for the Student Exchange Visitor Information System broken out by month.

Answer. Attached are fee projection charts for ICE by fee account for fiscal year 2006 versus fiscal year 2005.

Fee accounts	Fiscal year 2005	Fiscal year 2006
Immigration User Fee	$100,000	$101,621
Breached Bond Detention Fund	114,000	115,260
Student and Exchange Visitor Program:		
I–901 Revenues:		
October	1,459,215	2,039,431
November	2,636,660	2,166,852
December	3,451,620	3,135,481
January	2,211,365	2,092,676
February	1,970,220	1,485,072
March	2,661,321	2,661,321
April	4,452,487	4,452,487
May	6,211,727	6,311,727
June	7,225,460	7,509,932
July	7,149,570	7,441,213
August	4,515,573	4,524,954
September	2,072,375	2,072,375
Total	46,017,593	45,893,520
I–17 Revenues:		
October	30,659	1,050,960
November	27,960	403,680

Fee accounts	Fiscal year 2005	Fiscal year 2006
December	38,416	187,920
January	28,540	231,420
February	33,330	320,740
March	29,000	211,120
April	29,000	372,940
May	29,000	309,720
June	29,000	161,240
July	29,000	132,820
August	29,000	53,360
September	29,000	62,640
Total	361,905	3,498,560

Question. Please provide a chart with the fiscal year 2006 annualization projections broken out by fiscal year 2005 initiative.

Answer. Please see table below.

Enhancement	Annualization	One-time costs	Net
Compliance	$13,743	($9,710)	$4,033
IRP	28,478	(11,420)	17,058
Fugitive Ops	25,799	(11,543)	14,256
Alternatives	4,925	(2,856)	2,069
Bed Space	2,869	(1,326)	1,543
Backlog	13,256	(2,222)	11,034
Worksite	3,044	(1,648)	1,396
Total	92,114	(40,725)	51,389

Question. Please provide detailed comprehensive justifications for each program increase requested in the fiscal year 2006 President's budget.

Answer.

Homeland Security Data Network (HSDN)

[In thousands of dollars]

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 budget	Fiscal year 2006 change
ICE's portion of HSDN [1]	.....	.....	11,300	11,300

[1] Note: There is no base budget for HSDN. However, the Department's Working Capital Fund assessment for fiscal year 2005 is currently estimated to be $8.695 million. ICE contributed $3.2 million to the WCF in fiscal year 2004 for HSDN.

The fiscal year 2006 enhancement for HSDN totals $11.3 million and 1 FTE.

HSDN is a multi-agency, Department-wide project, funded from contributions from participating agencies. For fiscal year 2005, ICE's estimated contribution to HSDN is $8.7 million. In fiscal year 2004, ICE contributed $3.2 million to HSDN. Although ICE contributes funding for HSDN, the development, deployment, and management of the network is the direct responsibility of the HSDN Program Office which also manages all the funding for this ICE-sponsored initiative.

The HSDN is a secure communication network for transmission of information classified up to SECRET. It has been designed to replace several disparate legacy systems. HSDN will provide connectivity to the Department of Defense (DOD) Secret Internet Protocol Router Network (SIPRNet) to all users. DOD has indicated that non-DOD agencies should not use the SIPRNet as their primary classified communications medium. HSDN will provide access to SIPRNet via controlled gateways, satisfying this DOD concern. There are more than 400 DHS sites requiring HSDN deployment. Funding of this initiative will provide access to as many as 700 users in fiscal year 2006.

Funding for this request would support a HSDN coordinator to serve as a liaison between ICE program offices and the DHS's Science and Technology (S&T) Directorate, the HSDN program manager. The remaining resources would be provided to S&T for costs associated with the HSDN development process, including a survey of ICE locations, installation of equipment, set-up of terminals, and activation of service to terminals.

HSDN implementation was designed to follow a phased schedule. The first phase—which included the design and approval of the overall network design—has

been completed. The second phase proposes the installation of a limited number of terminals in 72 locations. Among these, 13 are ICE locations which include facilities within the Office of Intelligence and Office of Investigations. Equipment installation at these ICE locations is expected to continue through fiscal year 2005.

The remaining HSDN implementation phases will encompass the installation of all remaining locations including State and local offices. ICE has identified an additional eighty-eight locations which will have the HSDN installed in these remaining phases. These include the remaining Special Agent in Charge Offices, most Resident Agent in Charge Offices, Intelligence Collection and Analysis Teams, and remaining Office of Intelligence locations.

Performance Impact.—Funding of this initiative will provide access to HSDN as follows:

Performance increase	Fiscal year 2006 request level	Fiscal year 2007 request level	Fiscal year 2008 request level	Fiscal year 2009 request level	Fiscal year 2010 request level
Total number of HSDN users	700	1,000	1,000	1,000	1,000

Visa Security Unit

[In thousands of dollars]

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 base	Fiscal year 2006 budget	Fiscal year 2006 change
Visa Security Unit	.....	10,000	10,000	15,000	5,000

The fiscal year 2006 enhancement for VSU totals $5 million and 5 FTE.

The ICE Visa Security Unit (VSU) conducts in-depth review of visa applicants wishing to enter the United States, with the goal of denying visas to terrorists, criminals, and persons of special interest. Visa Security Program officers are assigned to posts to perform this law enforcement review of immigrant and nonimmigrant visa applications prior to visa issuance by consular officers of the Department of State.

For fiscal year 2005, the VSU's first year of funding, $10 million was provided to: (1) establish permanent operations in Saudi Arabia; (2) expand visa security operations to five additional high-risk locations (locations are not named here due to law enforcement sensitivity); and (3) hire 22 permanent positions (five at Headquarters and 17 at the overseas posts).

The enhancement requested for fiscal year 2006 would support nine additional positions ($4.827 million) and provide $173,000 for Investigations Training. These resources would advance incremental progress toward program expansion.

A $5 million enhancement to the base would:

—fund new overseas visa security post (to be selected based on current risk), staffed by three permanent Visa Security Officers, to expand the scope of visa security operations. Overseas operations involve: conducting in-depth scrutiny of high risk visa applicants; providing advice and training to consular officers to enhance their ability to detect terrorist, criminal, and otherwise fraudulent visa applicants through the consular adjudication process; and initiating investigations under DHS authority;

—hire two additional officers at Headquarters to provide operational and administrative support to the overseas operations;

—hire four permanent officer positions to replace temporary duty personnel currently investigating Security Advisory Opinions (SAOs) and "Section 306" cases (visa applicants from a State Sponsor of Terrorism);

—expand funding for Consular Training programs, including Headquarters consular training program development, Rapid Response Team capability, and consular evaluation program development.

Performance Impact.—The Homeland Security Act authorizes the Secretary of Homeland Security to assign employees of the Department to diplomatic and consular posts at which visas are issued, unless the Secretary determines that such an assignment to a particular post would not promote homeland security. The Secretary must submit an annual report to Congress that describes the basis for each determination that the assignment of an employee of the Department at a particular post would not promote homeland security.

Conducting the activities of the VSU in Saudi Arabia and expanding to the locations designated as highest risk by the Secretary are expected to generate an increase in homeland security outputs such as: recommendations to refuse individual visa applications, generation of investigative leads, additional lookouts and watch

list entries, identification of visa fraud schemes (including fraudulent documents, businesses, organizations, and associates), delivery of formal and informal training to consular officers, and other enforcement actions. The outcomes associated with these outputs may include a decrease in the vulnerabilities in the visa issuance process, increased integrity of the immigration system, and a greater awareness of terrorist suspects and activity patterns.

Performance level	Fiscal year 2005 est. level	Fiscal year 2006 request level	Fiscal year 2007 request level	Fiscal year 2008 request level	Fiscal year 2009 request level	Fiscal year 2010 request level
Percentage security review of all visa applications in Saudi Arabia	100	100	100	100	100	100
Percentage of high risk visa applicants scrutinized at the non-Saudi posts	NA					

Legal Proceedings

[In thousands of dollars]

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 base	Fiscal year 2006 budget	Fiscal year 2006 enhancements
Principal Legal Advisor	86,423	113,105	119,514	123,014	3,500

Note: Funding from the Salaries and Expense account only. Does not include reimbursable funding.

The fiscal year 2006 enhancement for Legal Proceedings totals $3.5 million and 24 FTE.

Of the fiscal year 2005 enhancements, 16 attorney and 12 support positions are scheduled for Headquarters while 38 attorneys and 8 support positions are targeted for the Field. The Headquarters positions will be distributed among existing Headquarters teams dealing with the following areas:

—Commercial and Administrative Law Division (primarily working on Merit Systems Protection Board appeals, and defending Equal Employment Opportunity claims generated by ICE clients (Federal Protective Service (FPS) and Federal Air Marshals (FAMS)), and handling bid protests primarily generated by FPS contracts;

—the National Security Law Division overseeing the litigation of national security cases, providing legal advice to the Office of Intelligence, and performing liaison activities with other law enforcement agencies;

—the Customs Enforcement Law Division, dealing with policy issues, and day to day monitoring of undercover operations, and ongoing criminal investigations; the Enforcement Law Division, dealing with a wide range of issues generated by the Office of Detention and Removal, the Office of Investigations, FAMS, and FPS, including statutory authority, search and seizure, use of force, and parole and custody issues, and the Human Rights Law Division, coordinating the litigation and advices the field on human rights abuser and persecutor cases.

The fiscal year 2005 field positions will be devoted to the following field areas:

—increased time and efforts spent on national security, predator and persecutor cases at the field level;

—increased training of staff on national security and persecutor issues;

—increased review of Notices to Appear prior to issuance or the hearing date;

—more timely movement of "change of venue cases" between district offices to cut down on adjournments because the agency representative does not have the file;

—increased amount of time spent on preparing a case for hearing, with a particular focus on review of alien evidentiary submissions and investigation thereof so as to minimize the number of adjournments required for document checks (by the Forensic Document Laboratory, the Department of States, and ICE/CIS offices abroad);

—increased emphasis on benefit and asylum fraud, including development of criminal prosecutions, so as to discourage the filing of fraudulent or frivolous applications;

—increased emphasis on responding to motions to reopen and filing responses to alien briefs before the Board of Immigration Appeals so as to diminish the number of non-meritorious cases that are reopened, and to speed up appeal processing at the Board of Immigration Appeals level.

These increased resources will also be used to assist the Office of Immigration Litigation (OIL) and the Offices of the United States Attorney (USAO) litigating Petitions of Review of removal orders and habeas challenges to custody and removal.

Past, current, and planned deployment of resources (Attorneys/Support):

	Current	Planned fiscal year 2005	Planned fiscal year 2006
Arlington	11/4	13/4	14/4
Atlanta	8/3	9/3	10/3
Baltimore	10/4	11/4	12/4
Boston (Includes Hartford Office)	19/6	21/6	23/7
Buffalo	8/3	8/3	
Chicago (Includes Kansas City Office)	17/7	19/7	
Dallas	10/4	10/4	
Denver (Includes Helena and Salt Lake City Offices)	11/5	12/6	12/7
Detroit (Includes Cleveland, Cincinnati Offices)	12/4	14/5	16/6
El Paso	10/4	11/4	12/4
Honolulu	2/1	2/1	
Houston	18/7	19/7	20/7
Los Angeles (Includes Las Vegas Office)	75/26	83/28	89/32
Miami	52/18	56/19	60/22
Newark	21/7	23/7	24/8
New Orleans (Includes Memphis Office)	14/5	16/5	17/5
New York	75/26	77/27	80/29
Orlando	11/4	12/4	
Philadelphia	15/5	16/6	17/7
Phoenix	22/8	25/9	27/9
St. Paul (Includes Omaha Office)	8/3	10/3	11/3
San Antonio (Includes Harlingen Office)	22/8	23/8	23/9
San Diego	25/9	25/9	
San Francisco	41/14	43/14	45/15
San Juan	3/2	3/2	
Seattle (Includes Portland and Anchorage Offices)	11/4	11/4	

EOIR's statistical data demonstrates that the largest pending case load exists in descending order in Los Angeles, Miami, New York, San Antonio (including Harlingen), San Francisco, Chicago, Boston (including Hartford), Orlando, Arlington, and Philadelphia Many cases from Harlingen are ultimately transferred through a change of venue order to more urban locations.

The specific results expected by the investment of resources and/or the impact of not providing the investment:

At present, six different entities (CIS—Asylum Offices and Examinations; CBP—Inspections and Border Patrol; ICE—Investigations and Detention and Removal) create the Notices to Appear (charging documents) that form the basis for litigation before the immigration court. With these expanded resources, ICE legal staff will be able to review more ICE generated charging documents to ensure better quality. It can also take more proactive steps to review charging documents created by other offices prior to the first master calendar on these cases, amending those charges that are legally deficient and filing such amended charges with the court in advance of the hearing date. This will lead to a reduction in adjournments. In addition, it will also permit the ICE litigation staff to terminate any cases that may have been improvidently brought.

Another source of adjournments (and hence backlog) stems from those cases where venue of the hearing has been transferred from one district to another. Frequently, because of a lack of support staffs, the needed files are not forwarded to the gaining office on a timely basis. With these added support resources, more focus can be made on those files, which are the subject of a change in venue, with either the losing office sending the file more expeditiously or the gaining office making more determined efforts to obtain the needed file in advance of the scheduled hearing date. These same support personnel can also more readily assist Assistant Chief Counsel in administrative tasks, which consume a great deal of attorney time best spent on moving a case forward.

The nature of immigration court litigation case has grown exceedingly complex. In the larger city offices, the vast majority of cases before the court are asylum claims, which are very time intensive to litigate. Unfortunately, asylum claims are frequently fraudulent and can be used by unscrupulous individuals as a way to gain status in the country. As part of the application process, aliens normally provide a

large number of documents in support of their claim, many of which may have been manufactured. To attempt to ensure the process is not abused, the Assistant Chief Counsel must conduct intensive alien file and document review. The Assistant Chief Counsel attempts to make full use of the Forensics Document Laboratory and other avenues of investigation to determine if the claim/documentation is bona fide. The Assistant Chief Counsel must also try to track down related alien files to determine if the alien has applied for a benefit under a different alien number/different name, locate alien files of relatives to determine consistency of the claim, and run extensive record checks. Assistant Chief Counsel also needs to contact victims in cases that are brought under the ICE Predator Initiative to assure that they are available to testify regarding the life long adverse impact these actions caused to them to assure alien sexual violators are removed and their relief applications are denied. With these additional attorney resources, Assistant Chief Counsel will be in a better position to do more complete and timely case review, and to request document checks, make record checks, and review related files in a timely manner. This in turn not only makes a better record on which the immigration judge can base his/her decision; it speeds up resolution of the case because all the crucial steps in the process are undertaken sooner.

Agency lawyers also work closely with the Office of the United States Attorneys, and Office of Immigration Litigation litigators by preparing litigation reports, reviewing records where remands are proposed, preparing recommendations for further review where judicial decisions are adverse to DHS interests and by providing guidance, advice and assistance on complex immigration law issues.

In a related vein, in larger city offices, ICE tries to have joint attorney-investigator focus on travel agencies and corrupt attorneys who actively encourage and assist in the filing of fraudulent or frivolous asylum cases. These cases clog the system and lead to additional court backlog. Currently, these joint attorney-investigator efforts have had to be more ad hoc and limited in nature. With these additional attorney resources, the staff would devote more time and effort to identifying the individuals who are the source of such claims, and work more closely with the criminal investigators in developing criminal prosecutions for the United States Attorneys Offices.

Temporary Worker Worksite Enforcement (TWP/WSE)

[In thousands of dollars]

Program	Fiscal year 2004 budget [1]	Fiscal year 2005 budget	Fiscal year 2006 budget	Fiscal year 2006 change
TWA	.....	5,000	23,000	18,000

[1] No funding was devoted to ''Temporary Worker Worksite Enforcement'' in fiscal year 2004, but approximately $18 million was devoted to Worksite Enforcement in fiscal year 2004.

The fiscal year 2006 enhancement for TWP totals $18 million and 72 FTE

As part of the President's proposed temporary worker program to match willing foreign workers with willing U.S. employers, enforcement of immigration laws to ensure compliance is required. Under the President's proposal, the temporary worker program would be open to new foreign workers, and to the undocumented men and women currently employed in the United States. The program would allow workers who currently hold jobs unlawfully to participate legally in America's economy, while not encouraging further illegal behavior.

The spend plan for the $5 million enhancement in fiscal year 2005 focuses on field training, employer outreach, and reconstituting the Worksite Enforcement Program infrastructure within the Office of Investigations in Headquarters in the final half of fiscal year 2005. Resources requested for fiscal year 2006 will primarily fund the deployment of FTEs to States (CA, TX, FL, NY, IL) having the greatest population of unauthorized workers.

The $18 million enhancement (of which $16.216 million is required in the Investigations Operations activity and $1.784 million is required in the Investigations Training activity) would fund 140 Special Agent and 3 support positions.

Performance Impact.—The additional resources will broaden the scope of the worksite enforcement program's strategic goals to include protecting the jobs and wages of legal workers by identifying and removing unauthorized workers. ICE will increase its presence at worksites, concentrating on employers in specific industries and geographical areas who intentionally violate the law or who have historically hired large numbers of unauthorized workers. ICE will also coordinate with Citizenship and Immigration Services to improve and expand verification services (Basic Pilot Program) to employers nationwide pursuant to the Basic Pilot Program Extension and Expansion Act of 2003.

Performance measure	Fiscal year 2006 request level	Fiscal year 2007 request level	Fiscal year 2008 request level
Administrative Worksite Case Completions	Base	+ 20 percent	+ 30 percent
Criminal Employer Case Presentations	Base	+ 20 percent	+ 30 percent

Organized Crime Drug Enforcement Task Force (OCDETF)

[In thousands of dollars]

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 budget	Fiscal year 2006 change
OCDETF	47,300	33,100	43,678	10,578

Note: In fiscal year 2004 and fiscal year 2005, OCDETF funding was reimbursable. In fiscal year 2006, funding proposed to be directly appropriated to ICE.

The fiscal year 2006 enhancement for OCDETF totals $43.678 million and 346 FTE.

Currently, funding for ICE OCDETF is provided on a reimbursable basis from the Department of Justice (DOJ). Beginning in fiscal year 2006, funding is being requested via direct appropriations to ICE. Funding requested would cover salary costs for 332 Special Agents ($41.840 million) and 14 Intelligence Research Specialists ($1.838 million) for a total of $43.678 million.

The Organized Crime Drug Enforcement Task Force (OCDETF) program is a Federal drug enforcement program that focuses attention and resources on the disruption and dismantling of major drug trafficking organizations. OCDETF provides a framework for Federal, State, and local law enforcement agencies to work together to target well-established and complex organizations that direct, finance, or engage in illegal narcotics trafficking and related crimes. Related crimes include money laundering and tax violations, public corruption, illegal immigration, weapons violations, and violent crimes. The OCDETF program has been in existence since 1982 and operates under the guidance and oversight of the Attorney General. Utilizing the resources and expertise of 11 member Federal agencies, along with support from State and local law enforcement partners, OCDETF has contributed to the successful prosecution and conviction of more than 44,000 members of criminal organizations and resulted in the seizure of cash and property assets totaling more than $3.0 billion.

No new FTEs are being requested. Rather, existing personnel will be paid by direct appropriation instead of by reimbursable funding.

In fiscal year 2004, ICE was reimbursed $47.3 million for costs associated with OCDETF. The reimbursable agreement for fiscal year 2005 provides for up to $33.1 million—a decrease of $14.2 million.

Performance Impact.—This initiative is intended to restore funding that was cut in fiscal year 2005, to ensure a consistent and more reliable funding source for ICE OCDETF activities, and to establish an appropriated base in lieu of reimbursable funding. This initiative is intended to provide funding that supports dedicated resources engaged in OCDETF activities and to maintain priority status for the program. The impact resulting from the decrease in reimbursable funding in fiscal year 2005 has ICE OCDETF requirements competing for funding—including priority status—within the ICE operational base. As a result, there can be no assurance that prior year performance levels can be maintained or achieved. Direct appropriated base funding is expected to support out-year ICE operations' planning that promotes the continued collaboration with other OCDETF participating agencies to achieve OCDETF goals and objectives.

$105 Million Base Increase for Investigations Operations

[In thousands of dollars]

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 base	Fiscal year 2006 budget [1]	Fiscal year 2006 enhancements [1]
Investigations Operations	796,478	1,138,495	1,099,554	1,267,437	167,883

[1] Note: The President's budget proposes enhancements of $167.883 million to the Investigations Operations budget activity. Of that amount, $105 million is a base increase, $4.827 million is for the Visa Security Unit, $16.216 million is for Temporary Worker Worksite Enforcement, and $41.840 million is for OCDETF activities.

The $105 million base increase will provide resources required to fund base requirements for the Office of Investigations, including salary costs, vehicle replacement, and other general expenses.

Performance Impact.—Improved infrastructure on which to support continuation of investigative activities, both domestically and internationally.

Detention Bed Space

[In thousands of dollars]

Program	Fiscal year 2004 budget	fiscal year 2005 budget	Fiscal year 2006 base	Fiscal year 2006 budget [1]	Fiscal year 2006 enhancements [1]
DRO-Custody Management [1]	550,912	697,855	594,169	727,769	108,600

[1] Note: There are three enhancements to the Custody Management program, totaling $90.0 million, $25.0 million, and $18.6 million respectively. The $25.0 million for ABC/Interior Repatriation is excluded in this display, as it is described separately.

The fiscal year 2006 enhancement for Detention Bed Space totals $108 million and 16 FTE.

The President's Budget requests an additional $90 million for detention bed space and $18.6 million as a base increase for the Custody Management program. Approximately $63 million of the $90 million is intended for the direct cost of providing an additional 1,920 beds. The balance of the $90 million request is intended to fund 32 new positions (16 FTE) to provide staff to support to those beds. This increase in bed space responds to increased demand for detention bed space generated by apprehending agencies (e.g., Border Patrol, Inspections, Investigations, etc.). The $18.6 million increase will provide resources required to fund base requirements for the Custody Management budget activity within the Office of Detention and Removal.

The fiscal year 2005 appropriation provided an additional $26.5 million for 1,216 new beds and 28 positions (14 FTE) above fiscal year 2004 levels.

Detention capacity and the necessary resources are fundamental components to the immigration enforcement mission. For the immigration enforcement mission to be successful, detention capacity must be considered at an appropriate ratio compared with resources provided for investigations and apprehensions. Increased detention capacity will improve the ability of ICE to verify alien identity, deter subsequent illegal entry, dramatically increase removal rates, prevent criminal aliens from returning to communities, and protect national security. Criminal aliens comprise more than half of the total detained population and we expect their numbers continue to rise due to enhanced enforcement efforts like IRP (Institutional Removal Program) and 287(g) expansion (local law enforcement authority to enforce immigration violations). Criminal aliens comprise a significant portion of our mandatory detention population (those individuals who have received final orders of removal and whose removal is imminent, those who are pending expedited removal activities, and those who are otherwise required by law or policy to be detained). In recent months, ICE's mandatory population has increased at a gradual, but steady rate due to increased enforcement activities (particularly from Expedited Removal initiative). As these targeted enforcement efforts continue, further growth in our mandatory detention population is likely. ICE continues to improve the efficiency of its detention program by consolidating populations and improving capacity management. These measures are anticipated to reduce costs by eliminating travel from detention facilities to proceedings, reducing average time in detention, and providing for more consistent and higher quality conditions of confinement for the detained population.

ICE will continue to enforce its robust facility inspection program and coordinate with our governmental organizations and non-governmental organization partners in pursuit of maintaining acceptable and appropriate conditions of confinement for the detained population. We are committed to effectively enforcing our immigration laws and protecting our Nation's security in a manner that affords the rights and proper treatment obligated under our laws to detainees, including those claiming asylum.

Fugitive Operations

[In thousands of dollars]

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 base	Fiscal year 2006 budget	Fiscal year 2006 enhancement
DRO-Fugitive Ops	26,916	44,687	48,121	57,001	8,880

The fiscal year 2006 enhancement for the Fugitive Operations is $8.88 million and 0 FTE.

The President's Budget requests an additional $8.88 million to support increased efforts to apprehend fugitive aliens. While estimates vary, the alien absconder population is more than 465,000 and that it continues to grow at a rate of more than

40,000 absconders per year. Experience with the current fugitive operations teams suggests that each team yields at least 500 absconder apprehensions/case closures per year. This success is very encouraging and expanding these efforts will stem the growth of the alien absconder population and begin to reduce the overall numbers of alien absconders at large.

ICE currently employs 16 fugitive operations nation-wide. Cities with fugitive operations teams include: Los Angles (2 teams), Boston, San Francisco, Miami, Houston, New York City (2 teams), Chicago, Newark (2 teams), Detroit, Atlanta, Baltimore, San Diego, and Seattle.

The fiscal year 2005 reprogramming request reduced the $50 million appropriated enhancement to $9 million. For fiscal year 2005, $9 million will support 42 full time positions (21 FTE) and additional funding for bed space and operating costs associated with increased apprehension activity.

This proposed enhancement is aligned to Department of Homeland Security Strategic Objective 2.2, Enforce trade and immigration laws.

All increases in removal rates increase the control DRO has over the removal alien population which contributes directly to national security.

Institutional Removal Program (Criminal Alien Program)

[In thousands of dollars

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 base	Fiscal year 2006 budget	Fiscal year 2006 enhancement
DRO-IRP	17,467	31,512	33,706	39,041	5,335

The fiscal year 2006 Institutional Removal Program (IRP) enhancement is $5.355 million and 19 FTE.

The President's Budget requests an additional $5.355 million to expand the IPR program and to continue the transfer of the program from the Office of Investigation to the Office of Detention and Removal Operations. The fiscal year 2005 amount will complete the transition of the State of New York and a sizable portion of the State of California. The fiscal year 2006 amount will continue the staffing of California.

IRP, now referred to as ICE's Criminal Alien Program (CAP), identifies aliens who are in criminal incarceration and processing them for removal prior to their incarceration release. This is an effective approach to preventing criminal recidivism and to ensure removable aliens are actually removed once so ordered by an immigration judge.

Currently, the ICE Office of Investigations administers the IRP program with a variety of resources (including job series 1811 criminal investigators). The workload for each immigration enforcement agent (IEA) is 300 charging documents served per year. This figure encompasses the number of interviews and record checks of individuals that are not amenable to removal but are of foreign birth. The plan for CAP is to interview 90 percent or more of all foreign born inmates in Federal, State and mega-county (populations over 1 million) areas. 287(g) (local law enforcement authority to enforce immigration violations) and video teleconferencing will serve the outlying areas.

ICE has placed increased emphasis on complex criminal investigations for its 1811 job series. In recognition of this, Congress provided an additional $30 million in the fiscal year 2005 appropriation to initiate the transfer of IRP from OI to DRO. The fiscal year 2005 reprogramming requests the enhancement be reduced to $4 million. This will allow for 37 positions and thus, Special Agents will continue to perform some institutional removal duties, instead of replacing all of them with Immigration Enforcement Agents (IEA). Criminal Alien Program (CAP) is the unification of the old Institutional Removal Program (IRP) and the Alien Criminal Apprehension Program (ACAP). All DRO activities in the incarcerated criminal alien arena will be referred to simply as CAP in the future.

STAFFING MODEL

Based on recent production numbers from New York State Department of Corrections (DOC) and Florida Department of Corrections, an IEA will in a year will do 600 interviews in Southern tier States and 500 interviews in Northern tier States. The statistics from these two DOCs suggest a higher percentage of naturalized foreign-born individuals in southern tier States requiring more interviews to obtain the goal of 300 charging documents issued per agent.

The transition will focus on a state-by-state transition of responsibility from OI to DRO. The first States, in order, are New York, California, Texas, Florida and Illinois. The transition, to date, is limited to the New York City Jail of Riker's Island.

New York.—The plan has been coordinated with NY State Department of Corrections and New York City Department of Corrections, the two largest non-Federal partners. Pre-existing system and partnerships with Executive Office for Immigration Review and Bureau of Prisons exist under legacy Institutional Hearing Program (IHP). Video teleconferencing will cover traditional ACAP locations at smaller county facilities. Equipment and staffing will be at newly completed Castle Point Facility which offers space for increased staffing.

California.—Plans have been discussed to improve the efficiency of identifying and starting removal proceedings for amenable aliens with the California Department of Corrections. The system is currently in a number of locations. Pre-existing system and partnerships with EOIR and BOP exist under legacy IHP. Video teleconferencing will cover traditional ACAP locations at smaller county facilities. Equipment and staffing will be hired and located to meet the needs of the State of California stretch the capacity of the New York VTC center. Due to the costs of installing VTC equipment to local detention facilities, the need will be relatively small in the first years and will be built up as demand grows.

Arizona Border Control (ABC)/Interior Repatriation

[In thousands of dollars]

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 budget	Fiscal year 2006 change
ABC	.....	.....	39,349	39,349

This fiscal year 2006 enhancement is $39.349 million for the ABC/Interior Repatriation Program. With this funding, the Interior Repatriation program will transfer from Customs and Border Protection to ICE/DRO in fiscal year 2006. DRO is in the business of removals and will use its experience to build on previous successes.

Interior repatriation (IR) is a component of the Arizona Border Control initiative (ABCI). ABCI is a multi-pronged approach to controlling the Arizona Border, which includes anti-smuggling investigations, fugitive arrests, as well as controlling and arresting illegal crossings. IR has a singular focus of the repatriating Mexican nationals. IR's aim is promoting deterrence, reducing recidivism of illegal crossings and thus reducing the number of deaths along the Arizona border.

In fiscal year 2004, 14,058 undocumented immigrants were voluntarily flown from Tucson, AZ, to the interior of Mexico from July 12 to September 30, 2004, after screening by DHS and a Mexican Consular Official. During the IR, Border Patrol Agents interviewed 96,793 potential candidates.

Of those interviewed, 82,735 refused to participate. Of those who declined to participate, 14,069 had been deemed "at risk" migrants. These migrants as well as the other migrants who refused to participate were processed either through voluntary return to the Arizona/Mexico border or other removal mechanisms.

A total of 7 percent (1,008) of IRP participants were arrested attempting re-entry into the United States during the IRP operation dates. This is much lower than the Tucson sector's average recidivism rate of 37 percent.

Interior repatriation can result in a dramatic reduction in the number of deaths in the desert suffered by intending immigrants. Interior repatriation efforts have resulted in strong U.S.-Mexico and cooperation. Since the IR pilot last year, DHS has also implemented expedited removal between ports of entry in the Tucson and Laredo sectors, resulting in additional apprehensions in the Tucson area.

Alternatives to Detention

[In thousands of dollars]

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 base	Fiscal year 2006 budget	Fiscal year 2006 enhancements [1]
DRO-Alternatives	8,659	12,202	12,733	23,533	10,800

[1] Note: There are two enhancements to the Alternatives to Detention program, each totaling $5.4 million.

The fiscal year 2006 enhancement for Alternatives to Detention totals $10.8 million and 7 FTE.

The President's Budget requests an additional $5.4 million to expand the Intensive Supervision Appearance Program (ISAP) and $5.4 million increase for the Alternatives to Detention program, for a total of $10.8 million in enhancements. Alternatives to Detention include intensive supervision, electronic monitoring, and telephonic voice recognition. Currently, ICE (through the Office of Detention and Removal Operations—DRO) is piloting several alternatives to detention initiatives.

Early indications are encouraging and suggest that these approaches to monitoring aliens who are not in physical custody may yield better appearance rates to immigration proceedings and better rates of removal once an alien has been ordered removed. The program is still too new to draw definitive conclusions. Over the next 6 to 12 months ICE will be collecting data and evaluating the efficacy of various alternatives to detention strategies.

ICE began piloting this initiative in fiscal year 2004 and has expanded the pilots in fiscal year 2005. Pilot cities include: Miami, Philadelphia, Baltimore, Portland, Denver, San Francisco, and others. The fiscal year 2005 Budget provided $11 million to expand the number of pilot locations and to fund 60 new full time positions (30 FTE). The fiscal year 2005 reprogramming reduces the funding to $2 million which permits funding for 11 new full time positions.

DRO will measure the performance of the ISAP program on three levels: (1) Do aliens enrolled in ISAP have a greater rate of appearance at hearings than the rate of a control group of non-detained aliens not enrolled in ISAP? (2) If ordered removed or granted voluntary departure, do aliens enrolled in ISAP surrender/depart at a greater rate than a control group? (3) If the alien fails to surrender for removal or otherwise fails to depart, are absconding aliens in ISAP re-apprehended at a greater rate than that for a control group?

DRO and its ISAP contractor are collecting certain data to test the hypothesis that the performance measures for aliens in ISAP will indicate a greater success rate than the performance measures for a control group of non-detained aliens. "Success" is defined as a statistically significant increase in the appearance rates, surrender rates, and re-apprehension rates. The hypothesis test will involve standard statistical tests (such as "t tests") and commonly accepted levels of statistical significance (generally the significance level in social science research is set to .05). DRO expects it will have gained a sufficiently large sample population to draw statistical inference within the next 6 to 12 months.

DRO and its contractor will also collect data on the appearances at hearings, surrenders for removal, departure from the United States, number of re-apprehensions of absconders.

The ISAP population is non-criminal aliens that are not mandatory detention, who live within a reasonable commuting distance of an ISAP office, and who agree to the conditions of the program. DRO will select a control group of non-detained aliens that are not participating in ISAP. These aliens will be selected from Docket Control Offices that have ISAP. The control group will closely match the ISAP group on such relevant characteristics as country of origin, gender, and length of stay in the United States.

General Explanation and Justification for the Initiative.—Detention of all aliens that are apprehended and placed into removal proceedings is not the only way to ensure that aliens appear at their immigration hearings or for removal. Aliens who disappear from ICE supervision pose a potential threat to public safety and national security. To mitigate this flow of cases into the fugitive population, ICE's DRO seeks to further develop alternatives to detention in two ways. First, expansion of the ISAP to two additional locations in fiscal year 2006. Each site is intended to accommodate 200 participants daily. These additional resources would bring the total number of participants nationwide on any given day to 2,000. The ISAP is a community-based, case management program that provides close supervision of illegal aliens emphasizing compliance with Immigration Court requirements. Expansion of the program requires 14 positions (7 FTEs). In order to properly execute the alternatives to detention program within DRO, positions must accompany program expansion. These positions will be used to manage the alternatives to detention docket including enrolling participants, managing the data, ensuring departure from the United States as required, and acting as the local Contracting Officer's Technical Representative.

This proposed enhancement is aligned to Department of Homeland Security Strategic Objective 2.2, Enforce trade and immigration laws.

Performance Impact.—This is a cost-effective way to ensure that aliens will appear for their immigration hearings or for removal. This program will increase the integrity of the immigration enforcement process by adding two additional ISAP locations, each intended to accommodate 200 participants daily. ICE is still analyzing the results of alternative to detention programs and will baseline the appearance rates in fiscal year 2006 to begin measuring the true outcome of ISAP. The goal of this program is in line with the strategic objective of removing all removable aliens. The anticipated increase in appearance rates will also mean fewer cases entering the fugitive population.

Federal Air Marshal Service (FAMS)

[In thousands of dollars]

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 base	Fiscal year 2006 budget [1]	Fiscal year 2006 enhancement
FAMS	610,290	662,900	678,994	688,860	9,866

This enhancement will allow the FAMS to increase its staffing level to a level that will allow it to meet its mission objective, the risk-based deployment of Federal Air Marshals. FAMS works closely with DHS and other Federal, State and local agencies and private industry to develop, deploy and sustain a comprehensive intelligence-driven approach and response to terrorist and related criminal threats against the United States and its interests. FAMS provides critical support to DHS' missions to prevent terrorist acts within the United States, reduce vulnerability to terrorism, and minimize damage from potential attacks.

Additional information can be provided in a secure manner.

Student and Exchange Visitor Program (SEVP)

[In thousands of dollars]

Program	Fiscal year 2004 budget	Fiscal year 2005 budget	Fiscal year 2006 budget	Fiscal year 2006 change
SEVP	1,465	40,000	[1] 58,100	[1] 18,100

[1] These numbers have been revised since submission of the President's budget on February 7, 2005.

DHS Strategic Objective Supported: 2.2 Enforce Trade and Immigration Laws

The Student and Exchange Visitor Program (SEVP) was created to restore integrity to the U.S. immigration system by ensuring that international students, scholars, and exchange visitors studying in the United States comply with the terms of their visas. One of SEVP's primary functions is to track the immigration status of foreign students and exchange visitors.

In fiscal year 2004, SEVP operated with two separate streams of funding—a fee collection process for school certification and appropriated dollars from counter-terrorism funds. The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 mandated the establishment and maintenance of a fee collection process to support the Student and Exchange Visitor Information System (SEVIS) and SEVP. To become a fully fee funded program, SEVP implemented a fee collection process (the SEVIS I–901 Fee) on September 1, 2004. This fee is paid by all prospective students and exchange visitors ($100 for most and $35 for some exchange visitors) prior to seeking a visa at the consulates and embassies overseas. The I–901 fee and the fees collected from schools seeking certification to host nonimmigrant students (I–17 Fee), provides the full funding for SEVP, portions of the Compliance Enforcement Unit (CEU), and the Department of State efforts.

In fiscal year 2005, SEVP projects it will collect $46 million from the SEVIS I–901 fee and $362,000 from the I–17 school certification fees. In addition, SEVP had a carryover balance of $2.6 million from fiscal year 2004. Although SEVP projects to have total resources of $49.0 million for fiscal year 2005, the execution level will remain at $40 million to ensure continuity of funding for the program.

In fiscal year 2006, SEVP projects to collect $45.9 million from the SEVIS I–901 fee and $3.5 million from the I–17 school certification fees. The increase in I–17 school certification fees is based on SEVP collecting initial fees as well as the re-certification fees whereas in fiscal year 2005 they will only collect initial fees. In fiscal year 2006 SEVP will have a full cycle of SEVIS I–901 fees since its inception in September 2004. SEVP projects to have total resources of $58 million for fiscal year 2006 that includes a $9 million carryover balance from fiscal year 2005.

FY 2004 carryover balance	$2,605,838	
FY 2005 collection estimate		
I-901A	$46,017,593	Estimate includes 5 months of actuals
I-17A	$361,905	
Total collections	$46,379,498	
Total balance	$48,985,336	
FY 2005 authority	$40,000,000	
FY 2005 carryover balance	$8,985,336	
FY 2006 collection estimate		Note: FY 06 Spend Plan @ $52,979,000
I-901A	$45,893,521	
I-17A	$3,498,560	
Total collections	$49,392,081	
Total balance	$58,377,417	
FY 2006 authority	$58,100,000	Note: FY 06 Carryover @ $5,398,417
FY 2007 collection estimate		
I-901A	$55,000,000	
I-17A	$4,000,000	
Total collections	$59,000,000	

The additional $18.1 million spending authority for fiscal year 2006 will allow SEVP to:

—Maintain staffing levels—the cost of salaries and benefits of newly hired employees

—Continue to improve SEVIS with IT enhancements—allows SEVP to accelerate the implementation of planned enhancements to improve the batch and real time interface processing, incorporate historical data from the SEVIS predecessor (CIPRIS) and implement a user-friendly reporting tool. This increase in funding will also allow SEVP to develop a search tool for the historical data.

—Conduct analysis of current fee structures (I–901 SEVIS fee and I–17 school certification)—fee studies for both the I–901 SEVIS fee and the I–17 school certification were conducted in early 2000

SEVP will continue to perform the following functions:

—Certify schools desiring to participate in SEVIS

—Provide law enforcement with current information on F, M and J nonimmigrants

—Conduct outreach to the academic community

—Accept and process fee payments

—Enhance the functionality of the SEVIS system

—Write policies and regulations to implement statutory requirements

—Train users of the SEVIS system

—Assist ports of entry, DoS consular officials, schools and program sponsors with the entry and stay of F, M and J nonimmigrants

Performance Increase	Fiscal year 2006 request level	Fiscal year 2007 request level	Fiscal year 2008 request level
Percent of F, M, and J nonimmigrant information maintained in SEVIS	100	100	100

Question. Are there any services that ICE is being assessed working capital fund charges for in fiscal year 2004 or fiscal year 2005 that are not directly utilized by ICE? Is ICE being charged for services on a basis proportionate to its usage?

Answer. According to the DHS Working Capital Fund reimbursable agreements, ICE will only be billed for actual services received. This was true for fiscal year 2004 WCF billings, and is expected for fiscal year 2005 billing. DHS provided detailed proration guidance with the fiscal year 2005 anticipated WCF billings. ICE agrees with DHS proration of WCF costs.

OFFICE OF SCREENING COORDINATION AND OPERATIONS (9/11 COMMISSION RECOMMENDATION)

Question. The President's Budget proposes to create the Office of Screening Coordination and Operations within the Border and Transportation Security Directorate. CIS has significant screening and identification capabilities and needs, yet the President's budget does not propose moving the operational responsibility for any of those programs out of CIS. In order to ensure that there is the closest possible coordination across screening programs, should CIS screening programs be moved to the Office of Screening Coordination and Operations?

Answer. The Office of Screening Coordination and Operations (SCO) is the first step in implementing the requirements of HSPD–11, which directs DHS to review and integrate all screening requirements across the Federal government. USCIS operational requirements and other security elements are being reviewed within the Department, and where deemed appropriate, may be incorporated within the purview of the SCO.

TERRORIST TRAVEL (9/11 COMMISSION REPORT)

Question. In addition to the formal 9/11 Commission Report, the Commission issued two staff monographs, one of them on Terrorist Travel. While no specific recommendations were made, the report reached interesting conclusions. One conclusion was that "Border inspectors today still do not have basic intelligence and operational training to aid them in detecting and preventing terrorist entry." They are not talking about people who are on watchlists, but providing inspectors with training to detect terrorists not on the watchlist. What steps is CBP taking to incorporate the information uncovered by the 9/11 Commission staff on terrorist travel into basic training for CBP officers?

Answer. CBP has established anti-terrorism response protocols to more effectively handle potential terrorism threats identified by CBP personnel. These national-level CBP policies operate both for a CBP Officer questioning a person applying for admission at a port of entry and for a Border Patrol Agent processing an individual who's been apprehended after crossing the border illegally to ensure consistent application throughout the border. CBP has also developed specific anti-terrorism training for passenger processing that includes specific instruction in behavioral analysis, deception detection and eliciting information.

The integrated curriculum for new CBP Officers includes three (3) specific components: Pre-Academy, Academy Basic training at Glynco, GA, and post-Academy training conducted at the Ports of Entry (In-port training). Academy Training courses for new CBP Officers include new anti-terrorism passenger training and fraudulent document detection. Most importantly, the role of an Officer in CBP's priority mission, anti-terrorism, is taught on day one and reiterated throughout the curriculum.

Under our new curriculum, our basic trainees receive 16 hours in fraudulent document training at the Academy that culminates with a graded practical exercise during which trainees examine characteristics of unique documents and determine if the documents are genuine, counterfeit or altered. The course highlights fraud indicators that may be present in evaluating any document for authenticity. Security features of United States entry documents and imposter detection are emphasized as well. Trainees that fail to successfully complete the course are removed from training. All instructors teaching this course have received training from the Forensic Document Lab.

With regard to questioning techniques, we use practical exercises throughout a trainee's 15 weeks at the Academy. With the help of role players, students are presented with scenarios based on primary inspection situations. During the labs and graded practical exercises, trainees review documents presented, question role players about their visit to the United States and make "refer or release" recommendations. Interviewing labs require trainees to practice observational skills and questioning skills, while applying their job knowledge of documentation requirements, immigration issues, customs exemptions, prohibited and restricted articles, and agricultural issues.

Question. Has CBP considered asking the 9/11 Commission staff to put together a seminar on its findings for all current inspectors, allowing them to sharpen their skills?

Answer. CBP is open to new training concepts, and though we are not sure that using former Commission staff for training CBP inspectors is an optimal approach, we will keep such ideas in mind as we continue to refine training programs.

Question. The report on Terrorist Travel also calls attention to the lack of "viable options to prevent documents known to be fraudulent from being returned to travelers denied entry into the United States". What additional authority would CBP need to be able to confiscate or in some way invalidate fraudulent documents prior to denying entry to someone?

Answer. U.S. Customs and Border Protection (CBP) implemented on January 1, 2005, under existing legal authority, a comprehensive program for the seizure and systematic processing of fraudulent travel documents presented for admission into the United States. Key parts of that program include the requirement that no fraudulent travel document be returned to the subject presenting the document and the mandatory forwarding of all seized documents to CBP's newly established Fraudulent Document Analysis Unit for intelligence collection and final disposition (return to issuing authority for destruction). Subjects from whom fraudulent documents have been seized are now issued a Single Journey Letter (SJL) to facilitate their return travel. The SJL conforms with all International Civil Aviation Organization (ICAO) Annex 9 standards for issuance of such documents. It includes interdiction and biographic information as well as the subject's photograph and fingerprints from both right and left index fingers.

Question. The report also states "There is no programmatic effort to focus on terrorist travel facilitators, and special agents lack the resources and authority to pursue visitors for immigration violations associated with terrorist activity". What is the Department's position on this statement? What can be done to change this?

Answer. ICE has special agents assigned to CBP's National Targeting Center (NTC), the FBI's Foreign Terrorist Travel Task Force (FTTTF) and the FBI's Terrorist Financing Operations Section. All three locations have developed specialized databases to facilitate the investigation of terrorist travel and terrorist travel facilitators. ICE Attachés assigned to posts around the world, and the ICE special agent assigned to the Department of Defense Central Command, are also well-positioned to act upon information relating to terrorist travel facilitators.

Question. One of the most interesting findings included in the report on Terrorist Travel, was related to the U.S. Department of Justice's Absconder Apprehension Initiative, started in 2001. Today, this initiative has become the responsibility of ICE's Fugitive Operations Program.

Of the almost 6,000 aliens determined to be the highest priority to track down and remove, 5 percent had been granted U.S. citizenship or had become legal permanent residents after being ordered deported. Can ICE and CIS guarantee that this can never happen again? What steps have been taken to ensure that this cannot happen again?

Answer. ICE works to ensure that data is shared and has developed and implemented agreements with CIS to share data. ICE also routinely runs CIS cases against the fugitive database. In addition, CIS has access to the Deportable Alien Computer System (DACS), which tracks all cases under removal proceedings.

Question. Is all of the relevant information that each organization has in its records being shared today? Is the Department confident that someone who has been ordered deported from this country can not be granted U.S. citizenship while an absconder?

Answer. The information regarding who is an absconder is readily available for queries and searches for CIS to determine if an applicant is considered an absconder or fugitive. An applicant for citizenship has the burden of establishing that he was lawfully admitted for permanent residency in the United States. The Naturalization application requires additional identity and security checks; a definitive response from the FBI background checks, and IBIS checks. In addition, all applications are processed in accordance with established Naturalization Quality Procedures (NQP).

Question. When someone is found to be attempting to fraudulently obtain U.S. citizenship, through the use of a false name or some other method, why does it take so long to bring them to justice?

On February 10, 2005, Mostofa Kamal, aka Shaheen Sardar, a native of Bangladesh, was arrested in New York. He entered this country in 1994, over 10 years ago. He was ordered to leave the United States in 1997. This individual made his first fraudulent request for benefits in 1997. Mr. Kamal was interviewed by CIS in connection with his application for U.S. citizenship in November of 2004, an application that was received by CIS in August of 2003, but he was only arrested 3 weeks

ago. The Department has known for sometime where he was—employed by the New York City Police Department as a Traffic Enforcement Agent. What is the issue? Is it resources, priorities? Why do these cases drag on so long before ICE arrests someone?

Answer. In the referenced case, the subject had previously entered the United States in 1993 under a false name and made claims to political asylum. His asylum claim was denied, and an Immigration Judge granted him Voluntary Departure with an alternate order of deportation should he not depart by the specified date in May of 1996. In 1997, he changed his name (name referenced in question), married a U.S. citizen, and applied for a benefit through that relationship. Based on that relationship, he left the United States, reentered, and was admitted to the United States as a Lawful Permanent Resident in 2000. He, in effect, caused an alternate order of deportation when he departed the United States to pick up his Visa. As a result of the name change, the fraud had not been detected. In continuance of this fraud, the subject applied for citizenship, for which he passed all stages in the process and was awaiting a naturalization date. The fraud was discovered. In February 2005, he was presented for criminal prosecution in the Southern District of New York for committing naturalization fraud.

It may take many years for an individual to exhaust his legal administrative remedies. Normally, arrests would not take place while there is an adjudicative or administrative judicial process being pursued and would only take place if the subject were considered likely to abscond. Generally, single scheme frauds are not accepted for criminal prosecution unless there are extraordinary circumstances that would sway the U.S. Attorney's office to consider it.

ARIZONA BORDER CONTROL INITIATIVE

Question. The Arizona Border Control (ABC) Initiative has been underway for almost a full 12 months. What are the results of this initiative so far? Has it been a success?

Answer. The Arizona Border Control Initiative (ABCI) has been very successful. Initial successes have established a foundation to expand on during fiscal year 2005 in order to achieve operation control of the Arizona/Mexico Border under control. Intelligence and arrest trends collected through ABCI indicate that alien smugglers have been forced to change their operating procedures as a result of ABCI. Selected statistics associated with ABCI are as follows:

—42 percent increase in arrests over the previous year
—105 percent increase in narcotics seizures over the previous year
—26 percent decrease in migrant deaths
—22 percent increase in Immigration Felony Prosecutions
—461 percent increases in vehicle seizures
—350 percent increase in weapons seizures

Question. What lessons from the ABC initiative can now be incorporated into the operations of CBP, ICE and others across the Nation?

Answer. Lessons learned that can be incorporated throughout the Nation include:

—Development of Planning Cell Committees of agency leadership personnel to coordinate the creation of operation plans to foster a seamless flow of information and to establish operating coalitions.
—Establishing a coordinated leadership structure with an emphasis on information and intelligence sharing and ensuring that sufficient resources are deployed is a requirement for success.
—Integrating operations between all BTS entities, State, local, tribal agencies and foreign governments achieve better results than working alone.
—Integrating ground-based surveillance technology, air surveillance, and ground personnel creates a "defense in depth" posture, which inhibits the ability of criminal enterprises to operate freely along the U.S./Mexico Border.

Question. Funding for this initiative has been requested in the fiscal year 2006 budget request. Should this initiative now be regarded as a permanent resource enhancement?

Answer. The $1 million increase included in the fiscal year 2006 President's Budget for the Arizona Border Control Initiative (ABCI) should be considered to be a permanent increase to CBP's base funding. These additional resources are required to meet the objectives of the ABCI.

Question. The use of unmanned aerial vehicles as a part of the ABC initiative has been considered very successful. However, the contract vehicle that the Science and Technology Directorate was using to provide the UAVs has ended, and there is no UAV coverage while CBP evaluates how best to continue this project. When does

CBP expect to have this issue resolved so that UAV coverage can be put back into place in the Tucson Sector?

Answer. CBP is currently refining requirements to issue a request for proposals (RFP) to the unmanned aerial vehicle (UAV) industry. The contract will specify delivery of the system within 30 days of contract award, which will allow CBP to establish a UAV initial operating capability on the Southern Border in support of the Arizona Border Control Initiative. CBP expects to award a contract for UAV procurement in the fourth quarter of fiscal year 2005.

ASYLUM AND EXPEDITED REMOVAL

Question. The United States Commission on International Religious Freedom recently issued a report entitled "Asylum Seekers in Expedited Removal". The report contains a number of recommendations for the Department of Homeland Security. The report raised specific issues on the difficulty of applying the standards for asylum and credible fear in a consistent manner across the Department. Has a working group or other mechanism been put in place to look into how the standards are applied and ensure consistent treatment of asylum seekers?

Answer. Since the inception of the expedited removal process in 1997, a standing inter-agency working group has addressed expedited removal issues. The Expedited Removal Working Group is an established forum for discussing all issues relating to expedited removal and comprises experts from each of the affected DHS entities (U.S. Citizenship and Immigration Services, Customs and Border Protection, and Immigration and Customs Enforcement).

Pursuant to former Deputy Secretary Admiral James Loy's concurrence with a joint memorandum from former Undersecretary of Border and Transportation Security Asa Hutchinson, USCIS Director Eduardo Aguirre, and Officer for Civil Rights and Civil Liberties Daniel Sutherland, the Expedited Removal Working Group has been tasked with coordinating review of the United States Commission on International Religious Freedom report, "Asylum Seekers in Expedited Removal." The working group also will draft the Department's responses to the report's recommendations. The working group will report on its review and proposed responses to BTS, USCIS, and CRCL, and their report then will be forwarded to the Secretary.

Question. The report also raised concerns about the detention policies and facilities used for the majority of asylum applicants. CBP, ICE, and CIS must all balance the national security needs of this country with the humanitarian needs of legitimate asylum applicants. In fact, almost at the same time that this report was made public, the 11th defendant in a significant case "Operation Jakarta" involving asylum fraud and document fraud pleaded guilty in a Federal court in Virginia. What is being done to review these programs and evaluate the specific recommendations of the Commission?

Answer. The Department of Homeland Security established a working group to review and respond to the recommendations suggested by the Commission. The working group will issue an evaluation on those recommendations this summer.

Question. What steps have been taken as a result of "Operation Jakarta" to track down anyone who received benefits fraudulently because of this criminal enterprise and remove them from the United States?

Answer. During the course of the criminal investigation, the USCIS Asylum Offices have reviewed 12,000 Indonesian asylum cases in order to identify all fraudulent cases related to "Operation Jakarta." Approximately 800 principal asylum cases were directly linked to the perpetrators of the fraud and will be processed for termination. Due to the high volume of fraud cases, the Asylum Offices have created teams of Asylum Officers to process the cases expeditiously. As the cases are terminated, the individuals will then be referred for judicial review to the Executive Office of Immigration Review (EOIR). All of the individuals that applied for and/or received benefits associated with this fraud will be entered as "lookouts" in the Treasury Enforcement Communications Systems (TECS).

USE OF STOLEN PASSPORTS—INSPECTOR GENERAL REPORT

Question. In December of 2004, the Department of Homeland Security's Office of Inspector General issued a report entitled "A Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States". Both ICE and CBP concurred with the recommendations in this report. What progress has ICE and CBP made to implement those recommendations?

Answer. ICE and CBP have implemented coordinated standard operating procedures to ensure ICE receives information on all individuals present in the United States who entered on a lost or stolen passport. On January 28, 2005, the Director of the National Targeting Center (NTC) sent the ICE Compliance Enforcement Unit

(CEU) a letter confirming the agreement between ICE and CBP. CBP will ensure lookouts are placed on all lost or stolen passports, conduct appropriate database queries, and forward information to the CEU on anyone present in the United States who entered on a lost or stolen passport.

Question. Please provide the Committee with a detailed, item by item, breakout of any fiscal year 2004 representation funds that were allocated to CBP, CIS, ICE, and the Under Secretary for Border and Transportation Security.

Answer. The requested information has been provided in the tables below.

Organizational element	Fiscal year 2004 appropriated	Fiscal year 2004 obligated
Office of Under Secretary for BTS	.....	.....
CBP	$40,000	$37,661
ICE	15,000	6,837
USCIS	5,000	4,953

FISCAL YEAR 2004 SUMMARY OF RECEPTION & REPRESENTATION FUND OBLIGATIONS

Date	Event	Amount
U.S. Customs and Border Protection		
30-Oct-03	Official luncheon held in honor of U.S./Mexico Border Partnership Meeting.	$381.14
13-Nov-03	Protocol Supplies	170.98
03-Nov-03	Refreshments served at the Operation Safe Commerce Meeting.	74.82
08-Nov-03	Sponsor the Ministers from Trinidad & Tobago at the Marine Corps Ball in Trinidad in furtherance of CMAA negotiations.	150.00
12-Nov-03	Refreshments for meeting hosted by Deputy Commissioner with Mexican Delegation.	21.09
17-Nov-04	Official Dinner in honor of Lars Karlsson, 2nd Deputy Director General, Sweden Customs.	402.82
19-Nov-03	Official Dinner with officials from New Zealand during CIS Discussions.	923.55
02-Dec-04	Official reception for the opening of the CSI Port in Durban, South Africa.	326.97
12-Dec-03	Protocol Supplies—Commissioner of Customs office	1,200.00
18-Dec-04	Official Reception hosted by Commissioner of Customs in honor of foreign dignitaries and high level officials from various Embassies.	10,523.50
21-Jan-04	Honorary Award Item for WCO Regional Security Conference in Senegal.	95.00
21-Jan-04	Official luncheon hosted by Chief De La Vina in honor of Mexican Officials, Fernando Creixell and Agustin Caso.	148.00
23-Jan-04	Official luncheon in honor of Canada Border Security Agency, President Alain Jolicoeur and Director Greg Boatbe.	213.68
28-Jan-04	International Customs Day Reception	3,473.00
29-Jan-04	Official dinner hosted by Secretary Ridge in honor of Canadian Prime Minister and delegation.	1,487.20
24-Feb-04	Official Luncheon for Italian Delegation during CSI Program Review.	608.00
03-Mar-04	Flowers sent on behalf of Customs and Border Protection upon the death of Comptroller of Customs, Robin Dare (New Zealand).	219.06
24-Mar-04	Official luncheon hosted by Acting Assistant Commissioner, International Affairs in honor of Mr. Kaci Abes, Director, External Cooperation & Relations.	125.13
22-Apr-04	Protocol Supplies for US/EU Signing	261.52
28-Apr-04	Official Luncheon hosted in honor of US/EU signing and the Joint Customs Cooperation Committee.	379.10
08-May-04	Protocol Supplies—Office of Trade Relations	10.60
13-May-04	Official luncheon hosted in honor of Mr. Mu Xin-Sheng, Minister, General Administration of China Customs and his delegation.	592.62

FISCAL YEAR 2004 SUMMARY OF RECEPTION & REPRESENTATION FUND OBLIGATIONS—Continued

Date	Event	Amount
24-May-04	Refreshments during meetings held with the European Community & U.S. Expert Groups on Container Security.	616.92
08-Jun-04	Dinner hosted by Commissioner Bonner in honor of the U.S./Canada Shared Border meeting.	450.00
08-Jun-04	Official luncheon hosted by Commissioner Bonner in honor of U.S./Canada Shared Border meeting.	514.30
08-Jun-04	Official Reception hosted by Commissioner Bonner at the U.S./Canada Shared Border Meeting.	1,967.06
14-Jun-04	Official luncheon hosted by Commissioner Bonner in conjunction with the U.S./Mexico Bilateral Meeting.	216.25
16-Jun-04	Official luncheon hosted by Acting Assistant Commissioner, International Affairs in honor of high level Georgian Officials.	562.50
22-Jun-04	Official luncheon hosted by Acting Assistant Commissioner, INA for the New Zealand delegation attending the WCO Policy & Commission meetings..	323.01
25-Jun-04	Official luncheon and toast hosted by Commissioner Bonner at the signing of the CSI agreement with the Hellenic Republic.	421.65
28-Jun-04	Official Luncheon hosted by Commissioner Bonner for high level French Customs officials.	495.00
14-Jul-04	Refreshments for CSI Global Targeting Assembly of Technical Experts Conference.	297.01
27-Jul-04	Official luncheon hosted by Acting Deputy AC, INA for attendees of the U.S./Australia Regional Movement Alert List System Conference.	878.41
04-Sep-04	Protocol Supplies—Director, Trade Relations	27.73
15-Sep-04	Refreshments during conference with Russian officials and CBP on Passenger Name Record connectivity.	106.60
22-Sep-04	Protocol Supplies—AC, INA and Commissioner Bonner's Office.	290.76
22-Sep-04	CSI PTP, Malaysia Luncheon	301.62
23-Sep-04	Honorary Award Items for Foreign Officials	8,404.74
Total Obligation		37,661.34
U.S. Immigration and Customs Enforcement		
11-Dec-03	Assistant Secretary Holiday Reception for members of Congress and other dignitaries.	1,325.89
3-Feb-04	International Attaché briefing w/light refreshments hosted by the Federal Air Marshal Services. Dignitaries and honorable guests traveled from Netherlands, Austria, Japan, China, Belgium, Egypt, Philippines, Brazil, New Zealand, Hungary, et.al.	717.75
2-Mar-04	Breakfast with Danish Minister at ICE	205.53
3-Mar-04	ICE One Year Anniversary Event attended by Captains, Chiefs of Police, State Police Officials, and representatives of other Federal Agencies.	299.06
20-May-04	Luncheon event for the Office of the Assistant Secretary with local officials and dignitaries who made substantial contribution to Nation or DHS.	416.75
8-Jun-04	Detention and Removal Operations Dinner during Four Country Conference in San Diego, CA to address mutual immigration and removal issues. Hosted by DRO; attendees included representatives from the Embassy of Australia; Canada Border Protection Agency; United Kingdom Immigration Service; and other foreign officials.	203.66
20-Aug-04	Opening ceremony for ICE Air and Marine Operations—Bellingham Branch; attended by U.S. Senator Patty Murray, U.S. Representative Rick Larsen, and other Congressional representatives.	490.00

FISCAL YEAR 2004 SUMMARY OF RECEPTION & REPRESENTATION FUND OBLIGATIONS—Continued

Date	Event	Amount
	Purchase of food and beverage items for AMO ceremony	476.08
18-Sep-04	ICE Air and Marine Operations briefing and site visit for Congresswoman Kay Granger and others. Includes purchase of refreshments for the event.	2,702.13
Total Obligation	.....	6,836.85
U.S. Citizenship and Immigration Services		
	Kitchenware supplies for Director's suite, for hosting VIPs and dignitaries.	389.07
	Honorary award items (coasters) for VIPs and dignitaries	998.93
	Official luncheon with dignitary Eduardo Ibarolla and Director Aguirre.	25.77
	Official dinner with incoming Mexican Ambassador Icaza and Director Aguirre to establish professional rapport.	220.96
	Honorary award item (Cufflinks) for guest speaker at USCIS 2004 Director's Leadership Conference.	79.95
	Honorary Award Items (Cufflinks) for senior representative and foreign dignitaries during official travel and visits.	1,075.95
	Honorary Award Items (Lapel Pins) for distribution by Director Aguirre during official travel and visits.	1,135.00
	Honorary Award Items (Pewter bowls and platters) for high-level dignitaries.	1,000.00
	Official Luncheon with senior-level guest (Alecia Casteneda) to establish professional interagency rapport.	27.52
Total Obligation	.....	4,953.15

SECURE ELECTRONIC NETWORK FOR TRAVELERS RAPID INSPECTION PROGRAM (SENTRI)

Question. In June of 2004 the Department of Homeland Security's Office of Inspector General (OIG) issued a report on the Secure Electronic Network for Travelers Rapid Inspection program, known as SENTRI. CBP agreed with the recommendations made by the Inspector General. Please provide an update on the progress that has been made in implementing each of the OIG's recommendations regarding the SENTRI program.

Answer. On January 24, 2005, a new Standard Operating Procedure (SOP) Manual was sent to the San Diego, CA, and El Paso, TX, Field Offices for the administration of the SENTRI program that addressed the majority of the recommendations in the OIG's report, including stating clearly the program eligibility criteria, establishing procedures for background checks and their resolution, developing minimum documentary requirements, separation of duties between initial enrollment and final approval, monitoring continued eligibility, and recording SENTRI violations. Certain other recommendations, relating to the Global Enrollment System and integration with related information systems are awaiting technical upgrades to achieve completion.

IMMIGRATION ADVISORY PROGRAM

Question. The Immigration Advisory Program is designed to improve border security against the threat of terrorism by enabling CBP to identify and intercept suspected terrorists and undocumented passengers before they board planes bound for the United States from overseas locations. The pilots established in Amsterdam and Warsaw in 2004 appear very promising. The fiscal year 2006 request includes funds to expand this program to two additional airports. Can, or should, this program be expanded more quickly?

Answer. Based on the results from Amsterdam and Warsaw through February 28, 2005, CBP believes the IAP should be expanded and has great potential for similar success at other large European, Latin American, and Asian hub airports. IAP expansion is dependent on reaching a bilateral agreement with the host country government and will be rolled out as expeditiously as possible while ensuring operational connectivity to port of entry operations.

Question. Please provide any evaluations or reports on the effectiveness of the IAP pilots.

Answer. Accomplishments for June 5, 2004, to February 28, 2005, for Amsterdam and September 5, 2004, to February 28, 2005, for Warsaw follow:

No Board Advisements	222
Fraud Intercepts	34
NTC Targets Confirmed	16
CBP Costs Avoided	$334,554
Potential Carrier Savings	$414,150

CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM

Question. The fiscal year 2006 budget requests an additional $8.2 million to expand the Customs-Trade Partnership Against Terrorism (C–TPAT). The fiscal year 2006 President's budget states that as of January 12, 2005, CBP had reviewed and accepted the security profiles of 4,460 companies, making these companies certified partners. The next step in the process is validation. According to information that was submitted for the record after last year's hearing, CBP planned to complete 400 validations of C–TPAT certified partners in fiscal year 2004. Was that goal met last fiscal year (fiscal year 2004)?

Answer. CBP initiated 500 validations and completed 287 during 2004. As of March 25, 2005, over 540 validations have been completed, with an additional 400 underway or in various stages of completion. CBP anticipates that over 900 validations will be completed by the end of fiscal year 2005.

In fiscal year 2004, CBP created a new position, Supply Chain Specialist (SCS), and sought to recruit qualified officers throughout the year. CBP continues to aggressively recruit permanent Supply Chain Specialists, and has trained field officers to help assist in the initiation of validations.

Question. What is the target number of validations CBP plans to complete in fiscal year 2005?

Answer. CBP will complete 500 validations in fiscal year 2005, for a total of 900 since the inception of program.

The overwhelming response by the trade community (volume of applications) forced CBP to reconsider the original goal to validate all certified members within a 3-year period.

CBP's strategy is for C–TPAT to determine and prioritize which sectors of membership will be selected for validations, selecting individual companies based upon a standardized risk assessment, and identifying "company specific" high-risk supply chains to better focus our efforts/resources.

Question. How many more validations will CBP be able to complete each year with the new resources that have requested?

Answer. The fiscal year 2006 request of $8.2 million will allow CBP to conduct as many as 600 more validation trips per year. Oftentimes, multiple validations are conducted on a single trip.

CBP anticipates having 100 Supply Chain Specialists (SCSs) on board by the end of fiscal year 2005. Each SCS is expected to complete 17 validation trips per year, with more than one validation conducted per trip. With 100 SCSs on board, CBP anticipates completing 1,700 validation trips per year. When fully staffed with SCSs, CBP could complete 2,669 validation trips per year.

Question. Last year, the Committee was informed that validations of foreign manufacturers would begin in calendar year 2004. Was that review of foreign manufacturers begun last year (calendar year 2004)?

Answer. During calendar year 2004, CBP initiated 500 validations of importers' foreign supply chains, which includes foreign manufacturers, and completed 287.

Validations of the Mexican manufacturer enrollment sector began in earnest in March 2005. Additional validations of Mexican manufacturers are being planned for June 2005.

AMERICA'S SHIELD INITIATIVE

Question. The President's fiscal year 2006 Budget includes a request of $19.8 million for the America's Shield Initiative (ASI). These funds will allow CBP to begin deployment of next generation technology for electronic surveillance along our Nation's land borders.

CBP is working on awarding a contract for the integration of ASI sometime this year. At the same time, CBP needs to operate and maintain the equipment that is in the field today. There are currently significant critical operational breakdowns,

cameras with unusable pictures, cameras down due to lightening strikes, camera control problems, cameras that have been replaced but are missing enclosures. In fact, the maintenance contract for the current installations lapsed in September of 2004, and CBP is still working on finalizing the replacement of those services. What is the plan to get the maintenance backlog taken care of?

Answer. As noted, CBP is moving ahead with plans to develop and implement the America's Shield Initiative (ASI), which will provide a more comprehensive, integrated solution to electronic surveillance the border. But simultaneously, CBP is still working to ensure that existing border surveillance infrastructure remains operational. For example, with regard to operational Remote Video System (RVS) installations in the field, activities are underway to address repair issues for operational sites. In addition, data and lessons learned from these current activities are being used to provide baseline data towards the development of an interim operations, maintenance, and repair program. This interim program will provide maintenance and repair support to existing field equipment pending the development and implementation of a maintenance and repair program that will support both existing and new field equipment.

Currently within CBP, the ASI Program Management Office (PMO), the National Emergency Equipment Repair and Maintenance Program (NEEMR), and the Tactical Communications Organization (TCO) have partnered to address several of these repair issues. For example, NEEMR, TCO, and the ASI (PMO) partnered to address the lightning strike incident that occurred at the Douglas, AZ Border Patrol RVS site. A team consisting of these three components responded to repair this installation. That activity was initiated at the beginning of February and concluded at the beginning of March. The result of this activity was the repair of the installation to a pre-lightning strike state, an assessment of current installation issues, and a collection of significant amount of baseline data regarding how these components worked together.

Question. When will the maintenance backlog be cleared up?

Answer. Establishing the ASI Program Management Office and the partnership with the National Emergency Equipment Repair and Maintenance Program (NEEMR) and the Tactical Communications Organizations (TCO), and awarding contracts for parts and equipment repair to original equipment manufacturers has significantly reduced the maintenance backlog. CBP believes that the maintenance backlog will be completely eliminated during the summer of 2005.

Question. This fiscal year, the plan for ASI calls for spending $10 million on surge technology. Please provide an explanation of what this is and what the plans are for this surge technology?

Answer. Surge technology is surveillance equipment that can be rapidly deployed in self-contained system packages that have the mobility and deployment capabilities to allow it to be positioned in a very short period of time to support changes in national operational needs. The plan at this time is to procure vehicle-mounted ground radar equipment that is co-mounted with a cooled, thermal imaging system that can sense and identify a vehicle as well as a human over 5 miles away. A system of this type will allow the detection and tracking of multiple items-of-interest and provides vectoring information to agents on the ground. By virtue of their mobility and transportability, CBP will be able to deploy these assets to the geographic regions or corridors that align with the current, nationally-assessed threat environment.

Question. CBP also plans to spend $10.6 million for replacement/repair of ground sensors in fiscal year 2005. Given that plans are in place to possibly award an integration contract to upgrade all of this technology, why are we replacing ground sensors now? Is it possible we will be replacing these again with something new in just a year or two?

Answer. In the early 1990's, the Federal Communications Commission (FCC) modified the spectrum range of commercial and government frequency usage. As such, CBP is required to change its systems to support the FCC frequency spectrum allocation requirements. CBP's Office of Border Patrol (OBP) is purchasing new unattended ground sensors to further augment its already deployed sensor fleet, to meet operational objectives, and to meet these FCC requirements.

An objective of this procurement effort is to ensure compatibility with any future systems that are acquired. Replacement of newly procured unattended ground sensors in a year or two is not anticipated. An objective of this procurement is to ensure that these sensors will readily integrate with future systems.

A cost analysis is being performed regarding the ability to upgrade our currently deployed unattended ground sensors that were procured and deployed prior to the FCC frequency spectrum allocation modification. This effort is also being under-

taken in such a manner as to ensure that these upgrades are made to meet FCC requirements and future systems integration.

Question. What is the timeline for initiating and completing all identified ground sensor repairs?

Answer. A proposal has been developed to augment sensor capabilities in Tucson Sector with 1,240 new digital sensors. As these sensors are deployed, the "old" sensors that are replaced, or rotated in from the field will, be assessed for redeployment to other Sectors as needed and in alignment with current enforcement objectives and national threat assessments. The project is scheduled to begin June 2005, with projected completion March 2008.

AUTOMATED COMMERCIAL ENVIRONMENT

Question. CBP has been working on modernizing the information technology systems that it uses for some time. The most significant project is the Automated Commercial Environment, known as ACE. Last year, CBP released the re-baseline estimate for completion of the ACE system. The new schedule has ACE being fully deployed in 2011, and costing an additional $1 billion. How confident is CBP that this new timeline can be accomplished?

Answer. CBP is confident the project can be completed in that time frame. That said, the new proposed baseline is presently under review. CBP will continue to strive to find ways to deliver ACE better, sooner, and at less cost. In addition, CBP has worked to improve ACE management. The staffs of legacy systems were merged into the CBP Modernization Office last December. The merger greatly increased the number of government staff on the program, as well as available subject matter expertise and IT project management skills. This will help keep the program on budget and schedule.

CBP now also has the advantage of working with an operational system. Release 3, implemented in June 2004, is fully operational and has already increased the amount of duty collected via Periodic Monthly Statement from $80,000 in June to over $109 million in February 2005. The Release 4 pilot in Blaine, Washington although currently experiencing some technical problems, has processed over 40,000 trucks. Having these ACE systems operating in "real-world" CBP environments provides excellent experience and feedback for the program team, and provides a solid base on which to build future capabilities.

Question. What is the status of the pilot in Blaine, Washington, of e-Manifest Trucks?

Answer. The ACE truck cargo/eManifest pilot was initiated in Blaine, Washington, on December 12, 2004. The system was very well received by the CBP Officers in the port, demonstrating a number of improvements over previous systems. However, system issues were uncovered, which caused delays in the processing of trucks. This resulted in a temporary halt to the pilot in late December in order to implement necessary changes.

The ACE pilot was re-started in mid-January with improved capabilities and significant streamlining of the cargo screening and release functions. With these changes, ACE has been processing trucks, on average, more quickly than the different release systems that had been in use prior to ACE. Average truck processing times were in the 70 second range.

Additional problems with the pilot were uncovered in early March. These problems were manifested as a result of the increased volume of trucks being processed (over 40,000 trucks had been processed with ACE). The problems have been corrected, and the revised system has been tested. Since the testing results were positive, CBP re-started the pilot April 4.

Part of the reason for difficulties with the pilot has been the low volume of electronic manifests submitted by carriers and service providers. A combination of difficulties with the CBP eManifest certification process and the effort required by the trade participants to make changes to their systems have led to the low participation. However, for those eManifests that have been submitted, ACE has performed extremely well, demonstrating the full promise of the system. CBP is working closely with the carrier community to increase, as quickly as possible, their use of eManifests.

CBP firmly believes that the current problems with the ACE pilot will be quickly corrected and the pilot will be operating successfully in the Port of Blaine. Plans have been developed to expand ACE to additional ports on the northern and southern land borders. Efforts are also underway to support 28 new carriers and service providers who have state their intentions to begin providing eManifests.

AIR AND MARINE OPERATIONS—RECAPITALIZATION

Question. A request for funding to begin the re-capitalization of the Border Patrol air fleet was included in the fiscal year 2006 budget, but there is no request for the replacement of Air and Marine's fleet. When can we expect to see such a request?

Answer. A program increase for re-capitalization of the Air and Marine Operations (AMO) fleet is not included in the fiscal year 2006 President's Budget, however, the fiscal year 2006 AMO base budget does include approximately $55 million for the procurement of replacement aircraft and deployment of new aircraft to CBP air wings.

Modernization of CBP air and marine assets is a priority in order to meet expanded missions in the areas of detection, surveillance, deterrence and apprehension, search and rescue, interdiction and Airspace Domain Security.

CBP is currently conducting a review of AMO and Border Patrol air and marine missions, operations and assets with the objective of determining how best to allocate and manage resources. It is anticipated that areas of both integrated and distinct aviation and marine missions will be defined, and opportunities for combining fleet modernization requirements will be identified. The existing AMO and Border Patrol modernization plans will be reviewed in the context of supporting the updated mission needs resulting from the transition analysis. All opportunities for commonality of aircraft, vessels, facility locations, command and control, maintenance and procedural standards are being reviewed. Potential benefits include enhanced threat engagement, procurement cost efficiencies, reduced life cycle costs, increased mission readiness and operational performance.

Development of a unified recapitalization plan for all CBP air and marine assets is will commence following completion of the integration.

WORKSITE ENFORCEMENT

Question. The President's budget requests $18 million for Immigration and Customs Enforcement (ICE) to double the resources devoted to worksite enforcement. The President's budget does not request any additional investigators for this program. Are there a sufficient number of investigators to pursue any leads or cases that may be developed?

Answer. ICE's fiscal year 2006 President's Budget requests $18 million for the temporary worker program to fund 140 agents and investigations training. It is proposed that the agents be assigned to field offices nationwide primarily to conduct employer audits, examine and prioritize leads, prepare and deliver Notices of Inspection and Notices of Inspection Results, and develop employer cases involving administrative fines. Agents would be assigned to field offices in the States with the greatest number of unauthorized workers.

The requested resources would enable ICE to increase its presence at worksites in specific industries and geographical areas, concentrating on employers who intentionally violate the law or who have historically hired large numbers of unauthorized workers.

Question. Please provide the Committee with a description of ICE's current worksite enforcement program, including what authorities are being enforced and how the program is run.

Answer. ICE worksite enforcement program activities focus primarily on removing unauthorized workers from critical infrastructure facilities to reduce the risk of terrorist attack from insiders. This may be accomplished through screening and arrest operations to identify and remove the unauthorized workers, as well as through strategic partnering with employers and the law enforcement entities controlling facility access. ICE worksite enforcement activities also target criminal employers whose violations have a nexus to human smuggling, immigration document or benefit fraud, and worker exploitation.

The authorities being enforced generally include one or more of the civil and/or criminal provisions of INA 274A (Unlawful Employment of Aliens). Many criminal employer investigations also charge violations relating to harboring, smuggling, and document fraud.

Question. Please provide the Committee with a breakout of worksite enforcement workload of administrative cases versus criminal investigations for fiscal years 1999 through 2004, including a breakout of the FTE devoted to this area by type of employee for those same years.

Answer. Please see table below.

Performance category	Fiscal year					
	1999	2000	2001	2002	2003	2004
Criminal Employer Cases	[1] 182	[1] 109	[1] 239	[1] 21	[1] 4	[3] 59
Notices of Intent to Fine Issued	[1] 443	[1] 213	[1] 141	[1] 73	[1] 16	[1] 3
Number of Fines Collected	[4] 890	[4] 478	[4] 292	[4] 115	[4] 54	[4] 64
Fine Amounts Collected	[4] $3,690,575	[4] $2,234,181	[4] $1,599,323	[4] $509,835	[4] $212,322	[4] $118,528
Worksite Arrests	[5] 2,849	[5] 953	[5] 418	[6] 816	[6] 505	[6] 642
Investigative Work Years (Work Year=1,695 hours)	[5] 278	[5] 202	[5] 134	[5] 152	[5] 105	[5] 90
Case Completions	[5] 3,844	[5] 1,966	[1] 1,595	[1] 2,061	[1] 1,490	[7] 523

[1] Source: LYNX.
[2] Source: TECS.
[3] Calculated utilizing Treasury Enforcement Comms System(TECS) records (criminal employer cases opened).
[4] Source: Debt Management Center.
[5] Source: PAS.
[6] Manually calculated utilizing internal reports submitted by field offices.
[7] Manually calculated based upon the number of completed cases in LYNX and the number of cases reported closed in TECS.

VISA SECURITY UNIT

Question. The President's budget requests an increase of $5 million to expand the Visa Security Unit. The recently submitted "Visa Security Program: Annual Report for 2003–2004" talks about the critical need for coordination and training with the Department of State Consular Affairs and CBP. What mechanisms are in place to ensure that there is the closest possible cooperation in this program?

Answer. The Visa Security Program (VSP) within ICE is responsible for implementing Section 428(e) of the Homeland Security Act, which calls for the deployment of DHS officers to visa-issuing posts, unless such a deployment would not benefit homeland security. One of their principal duties under Section 428(e)(1) is to provide advice and training to consular officers regarding specific security threats relating to the adjudication of individual visa applications or classes of applications. DHS Visa Security Officers in Saudi Arabia are currently providing this training, and upcoming deployments of Visa Security Officers will expand this activity to additional posts. In addition, ICE and the Department of State have designated points of contact at Headquarters who coordinate closely on issues including consular training. A representative from the Visa Security Program has briefed each graduating class of consular officers since October 2004.

VSP also coordinates with CBP on several operational levels. Visa Security Officers regularly utilize the National Targeting Center as a supporting element in their in-depth review of visa applications. In addition, CBP officers have served temporary details at Headquarters and in the field. Finally, VSP has opened announcements for permanent positions to both ICE and CBP officers in order to recruit officers with a full range of immigration enforcement skills to serve overseas as Visa Security Officers.

The President's requested increase of $5 million in fiscal year 2006 will fund expanded VSP operations in the field and at Headquarters, to include its consular training responsibilities.

Question. In August of 2004, the Department of Homeland Security's Office of Inspector General issued an evaluation of DHS activities to implement section 428 of the Homeland Security Act of 2002. This evaluation included a number of recommendations to improve the workings of the Visa Security Officers. What is the status of implementing each of the recommendations in that report?

Answer. Since the DHS Inspector General's (IG) evaluation in late 2003, shortly after the initial deployment of officers to Saudi Arabia, Visa Security Program operations in Saudi Arabia have made significant progress. Of the IG's twelve recommendations, three had been closed at the time of the report's publication. The remaining nine recommendations were resolved, and remain open while they are implemented. Below is an update on each of the IG's recommendations.

Recommendation 1.—Develop a curriculum of homeland security training for consular officers consistent with the requirement in Section 428(b)(1) of the Act.

ICE is working to develop homeland security training for consular officers. A VSP's program development staff member has attended the Basic Consular Training Program at the Department of State's (DOS) National Foreign Affairs Training Center (NFATC) as a basis for ICE's recommendations to DOS about consular training. VSP staff also held a curriculum development conference with training experts from the Federal Law Enforcement Training Center (FLETC) and ICE Academy to plan the development of the consular training program. Since October 2004, VSP leadership has been addressing each graduating class from the Basic Consular Training

Program, to introduce them to the visa security mission and to prepare them to work with Visa Security Officers in the future.

Recommendation 2.—Develop a training program for Visa Security Officers (VSOs) that includes foreign languages, country studies, and interview and fraud detection techniques.

Working with the ICE Academy and FLETC, VSP developed a 4-week training curriculum for Visa Security Officers, incorporating the IG's content recommendations. With specific regard to language training, ICE's VSO selection criteria will continue to emphasize language ability, and VSP will continue to exercise best efforts to provide additional language training where necessary.

Recommendation 3.—In coordination with DOS, develop performance standards to evaluate consular officers.

ICE continues in an audit capacity, to advise DOS on consular performance evaluation. A VSP staff member recently attended Basic Consular Training to assess how consular officers currently are trained and evaluated.

Recommendation 4.—Develop written criteria for assigning VSOs to other countries.

Closed. ICE established such criteria in early 2004, and the OIG closed this recommendation as it published the report in August 2004.

Recommendation 5.—Assign responsibility to develop and publish the report to Congress required by Section 428(e)(4).

ICE/VSP will prepare the report, and BTS will submit the report to Congress.

Recommendation 6.—Conduct a study of the personnel management techniques used by other agencies with a global workforce and evaluate ways to facilitate the overseas rotations of DHS employees.

DHS is continuing to evaluate its international presence. No specific policy recommendations have yet been announced.

Recommendation 7.—Discontinue the practice of filling the VSO positions with temporarily assigned officers and move toward filling the positions with permanently assigned officers.

VSP has announced and selected positions for Saudi Arabia. VSP will announce permanent positions for all future offices.

Recommendation 8.—Establish criteria for selecting VSOs based on required experience and skill sets to support the visa security operation.

Closed. ICE established such criteria in early 2004, and the OIG closed this recommendation as it published the report in August 2004.

Recommendation 9.—Establish a funding mechanism to ensure that the visa security operations receive all required support and that DOS is promptly reimbursed for the support that it provides.

VSP has received funding in fiscal year 2005 for its existing posts in Saudi Arabia and for expansion to four additional locations. This will become the base for fiscal year 2006 and the out-years for all locations opened in or already in operation as of fiscal year 2005. To facilitate administrative coordination, DOS and VSP recently signed a Memorandum of Agreement that explains how reimbursements and other administrative matters will be handled.

Recommendation 10.—Propose a technical correction to Section 428(i) to align it with Section 428(e) and permit DHS to review only those applications with homeland security interest in Saudi Arabia.

Closed. The OIG agreed with ICE's position that the legal requirement to review all visa applications in Saudi Arabia should not be modified. The OIG closed this recommendation as it published the report in August 2004.

Recommendation 11.—Evaluate the possible benefit of analyzing the existing visa applications in DOS files of young Saudi males who were issued visas in the 2 year period prior to September 11, 2001. BTS should coordinate with DOS, the FBI, and other Federal agencies, as necessary, before making a determination about whether, or how, to proceed to analyze the applications.

ICE agrees that there may be value in reviewing certain applications submitted in Saudi Arabia in the 2 years prior to September 11, 2001. DHS is still evaluating whether or how to proceed with such an analysis.

Recommendation 12.—Develop an interface between BTS and DOS computer systems that permits a fast and efficient method to automate the visa security name check process and eliminate the duplicative data entry for database checks.

ICE has been working with DOS to improve information sharing and access and has succeeded in virtually eliminating the manual data entry that the IG observed in late 2003/early 2004. VSP is working with DOS to further enhance regular information sharing and expects the new process to be in place in the third quarter of fiscal year 2005.

OVERHEAD COST SHARING

Question. Last fiscal year and this fiscal year, ICE plans to charge a portion of the headquarters overhead costs to the Federal Protective Service (FPS) and the Federal Air Marshals (FAMS). On what basis were the overhead charges calculated to ensure that those organizations were paying for services they received on a basis proportionate to their usage?

Answer. Early in the fiscal year, FPS and/or FAMS were expected to provide funding for overhead based for the actual costs for services. The headquarters (HQ) overhead costs are allocated to the ICE components using full-time equivalents (FTE), at the beginning of the fiscal year, to construct the proration percentages. Following a review of the overhead costing issue for the FAMS and FPS, a final decision was made that the FAMS and FPS would only pay for services actually being utilized. However, they will not be assessed an overhead charge in fiscal year 2005.

Question. Will this become a permanent charge to FPS and FAMS? If so, why are no additional resources being requested to ensure that the funds are available to pay these bills?

Answer. All ICE Programs, Projects and Activities (PPAs) should be expected to share HQ overhead costs for the overhead services that ICE provides. However, for fiscal year 2005 there will not be an assessment for FPS and FAMS.

HQ overheads are covered out of base appropriated funds. Additionally, every new enhancement request includes funds for HQ overhead in the modular costs used to compute the enhancement.

Question. Will this have an adverse impact on the ability of the FAMS to maintain its staffing levels?

Answer. No, the FAMS are not being assessed an overhead charge.

FUGITIVE OPERATIONS

Question. The President's budget requests an increase of $8.8 million to expand the capabilities of the fugitive operations teams. In answer to questions submitted after last year's hearing, ICE stated that the strategic plan called for the elimination of the 400,000 fugitive backlog within 10 years based on significant increases in the fugitive program.

What impact are the continued funding shortfalls having on the Office of Detention and Removals' ability to implement that plan?

Answer. ICE continues to track and apprehend fugitives and continue to surpass goals and previous year's statistics. However, some existing teams need additional staff that have not yet been hired, and no new teams have been deployed. When corrected later this year, this delay will have no effect in meeting the 10-year plan.

Question. Does the fiscal year 2006 budget request include sufficient resources for ICE to continue making progress in locating and deporting absconders?

Answer. Yes. The fiscal year 2006 Budget will allow ICE to show significant progress in locating, apprehending and removing absconders.

Question. Has ICE been able to move ahead with the data integrity projects related to the absconder records despite the funding situation? What results have been seen from the data integrity projects?

Answer. ICE has been investigating data integrity issues with the records of absconders. ICE drew random samples of records of aliens with an unexecuted order of removal that did not indicate that the alien was an absconder. There are approximately 130,000 such alien records (does not include aliens with an acceptable reason for an unexecuted order). The samples indicated that almost 70 percent of those aliens were absconders. The absconder statistics have been revised accordingly. DRO estimates that the absconder population on September 30, 2004, was 465,353 aliens.

ICE believes that the new data system to track aliens in removal proceedings (EREM) will address many of the data integrity concerns. The data system will be easier to use which will encourage completeness and accuracy. It will also be more tightly integrated with the work process used in an alien's case.

FEDERAL AIR MARSHALS

Question. On January 27, 2005, ICE announced the creation of the Federal Air Marshals (FAMS) Advisory Board. The advisory board will provide information and recommendations on key FAMS policy and operational issues. Some of the issues the FAMS Advisory Board will initially address are hiring, dress code, technology, the FAMS role in airport security and the FAMS career ladder within ICE. When does ICE expect that the advisory board will begin making recommendations on some of these issues?

Answer. While it is difficult to predict with specificity when the FAMS Advisory Board will be prepared to make recommendations, the Board is currently meeting on a regular basis. One of the objectives of the Board is to increase the pace of the FAMS integration into ICE. To that end, the Board hopes to be in a position to make recommendations in the near future.

INSTITUTIONAL REMOVAL PROGRAM

Question. What progress has been made in transitioning the Institutional Removal program from the Office of Investigations to the Office of Detention and Removals?

Answer. In the planning for the transition of responsibility from the Office of Investigations (OI) to Detention and Removal Operations (DRO), a review of performance standards and available resources was completed.

This review found less than 50 percent of criminal aliens were being identified and removed from the United States (comparing State Criminal Alien Assistance Program (SCAAP) numbers to the Performance Analysis System (PAS)).

The prior performance standard based on the number of aliens removed is not reflective of the function of the Criminal Alien Program (CAP). The performance standard for DRO will be the percentage of incarcerated foreign born screened for removal. A performance level of 90 percent of all foreign-born incarcerated in Bureau of Prisons, State department of corrections and mega-counties (areas with populations over 1 million) will provide a high level of coverage throughout the United States. Smaller population areas would be encouraged to participate in 287(g) programs or video teleconferencing with newly established VTC centers.

After careful consideration, DRO determined that a state-by-state approach would be the most effective way to ensure a successful transition. By approaching the transition on a State level, staffing plans and proactive communications with relevant State agencies can enhance the productivity and workflow.

The State of New York was determined to be the first State to transition because of the existing work force available in DRO to assist in covering the City of New York. DRO assumed sole responsibility for the City of New York Department of Corrections (NYC DOC) on December 17, 2004. With ten facilities, one satellite facility in Bronx, 120,000–130,000 inmates admitted annually and with an average daily population of 15,000, NYC DOC is one of the largest detention programs in the United States.

The transition at NYC DOC has been remarkably smooth and in the first quarter of fiscal year 2005, improvements have been substantial. In the last quarter of fiscal year 2003, prior to the transfer, 921 of 3,542 incarcerated aliens were screened (26 percent). In the first quarter of fiscal year 2005, there were 1,866 of the 2,696 incarcerated aliens screened (69 percent). Though well below the stated performance level; significant progress has been made without additional staffing. As staffing becomes available, NYC DOC operations will achieve the target level of screening.

The State of New York effort has provided an excellent blueprint for subsequent transfers, and using the lessons learned, DRO has completed transfer plans for California, Florida, Illinois, Arizona and New Mexico.

Question. Are there other ways ICE could be working with State and local officials to improve communication in order to identify incarcerated aliens in a more timely manner?

Answer. In the planning for the transition of responsibility from the Office of Investigations (OI) to Detention and Removal Operations (DRO), a number of possible communications enhancements have been explored by DRO.

The most basic approach to improve communications is and continues to be open, face-to-face dialogue with the local and State officials to determine the needs and requirements of both parties, to establish an approach to accomplish the mutual goals, and to maintain an open line of communication between the parties.

During the planning for the State of New York, ICE met with State officials that oversee the entire New York State Department of Corrections, Parole and Probation and the State Police. These discussion have led to an enhanced streamlined approach to processing aliens, centralized release of aliens to ICE custody, created a procedure for State of New York Parole to compare information and update their information based on removal information and opened the dialogue to continue improvements in the areas of conviction documents, appeal processes in State courts and new procedures for automated immigration status checks. Dialogue has already been started with the State of California and a meeting between ICE/DRO and the Assistant Chief of Staff of the Governor's office has been planned for the end of March.

ICE has also investigated whether the 287(g) program by State and local governments is another opportunity to train local law enforcement in the authorities as well as what the information provided to them means. The Immigration and Nationality Act (INA) and supportive data bases can be confusing to experienced officers, much less individuals that have not had years of experience in these issues. The formalized training allows for concise communication of status to ensure proper enforcement of the INA. Expansion of the 287(g) program has a direct impact on the DRO program through the additional identification of individuals amenable to removal.

The PEGASUS program is operated under a COPS grant and allows a new venue to share information with local and State authorities. The program provides Sheriffs and municipal law enforcement with secure access to other participating law enforcement agency databases. Through recent presentations, DHS is considering how best to incorporate parts of our databases to assist identification of aliens amenable to removal as well assist DHS in our mission. The databases in question would definitely include the Deportable Alien Control System (DACS) and would allow an automatic data search system via a "pointer system". The possibilities of an automated system would greatly enhance the identification of aliens in removal proceedings and those already removed. The extent of the data sharing that DHS is willing to consider is still under review.

The Law Enforcement Support Center (LESC) continues to provide a one-stop location for searching several data systems. The LESC, currently operated by OI, accepts queries from a multitude of law enforcement agencies and sends responses back to the originating agency. In cases where the alien in question is identified as a removable alien, a detainer is placed by the LESC for the local DHS office to pursue appropriate removal action.

FEDERAL PROTECTIVE SERVICE

Question. The Federal Protective Service (FPS) has been in the midst of a very difficult transition from the General Services Administration's (GSA) financial management system to that of ICE.

Given the financial problems of ICE, which extend to not having proper internal fund controls, why wasn't more consideration given to having FPS continue to use the GSA financial system for at least 1 more year, or until eMERGE2 was ready?

Answer. The Department of Homeland Security, Office of the Under Secretary for Management, initially directed that the FPS transition from the GSA financial management system be completed by October 1, 2003. Following the initial review of the unique financial management requirements needed to support the FPS offsetting collections program, the transition date was extended to October 1, 2004. At the time that this decision was made, ICE felt that the additional year for planning the transition would be sufficient to avoid any major problems. The GSA and ICE Financial Management staffs worked closely to plan for a smooth transition. However, the technical financial and accounting differences between the GSA and ICE financial systems proved to be much greater than either agency had anticipated. The ICE Financial management staff has been following an aggressive plan and timetable to complete the FPS transition by September 30, 2005.

With regard to the specific financial situation, specific planning milestones called for a successful transition of FPS to ICE, as agreed with GSA, FPS and ICE. This plan was successful, with the only contributing factor being data transmission problems from GSA. That situation exacerbated payment problems in the ICE transition. Much of the data from the GSA financial system has had to be manually uploaded into the ICE system, requiring additional quality assurance steps to maintain the highest level of data integrity.

Question. The current remediation plan for fixing the financial problems at FPS call for the reconciliation of payments to be finished by March 31, 2005. How will this plan solve all of the problems and ensure that contractors will get paid in a timely manner?

Answer. In addition to a full reconciliation of FPS payments, ICE is convening a high level working group to address the financial problems at FPS. This group will evaluate and make appropriate changes in the business process flow to ensure that contractors are paid timely and that financial events are properly and timely recorded. ICE will continue to work with GSA to resolve any discrepancies in the balances transferred. A full reconciliation of financial activities is anticipated by September 30, 2005.

HUMAN SMUGGLING

Question. What is ICE doing in the area human smuggling? What has happened in the Carreto case that was the subject of a recent CBS News report?

Answer. Recognizing that global human smuggling is of the nature of organized crime, ICE has employed Task Force methodologies to attack and dismantle the operations and networks that profit from these crimes. An example of this methodology is Operation ICE Storm in Phoenix, Arizona. ICE, in conjunction with partners in the Federal, State, local and foreign law enforcement community, has initiated a task force to address widespread violence, kidnapping, extortion, and other crimes associated with human smuggling. By vigorously applying its money laundering authorities, ICE and our State and local and partners in Arizona have deprived human smuggling organizations of nearly $7.3 million of their criminal proceeds. Since the inception of ICE Storm in October 2003, over 320 persons have been prosecuted for human smuggling and related crimes and over 170 firearms have been seized. Over 6,700 smuggled aliens have also been arrested and removed from the United States.

ICE is fully supporting the Arizona Border Control (ABC) Initiative, which was developed to focus on criminal organizations and supporting infrastructures that are currently exploiting the Arizona region. ICE's role in this initiative, which is being coordinated closely with other BTS components as well as State, local and foreign law enforcement agencies, focuses on interdiction and investigation efforts to target human and contraband smuggling organizations operating near the Arizona/Mexico border. To date, a total of 635 individuals have been prosecuted as a direct result of those enforcement efforts. In addition to what has already been seized under ICE Storm, approximately $2.1 million in U.S. currency has been seized and 26 weapons have been removed from the streets.

Since July 2004, ICE has implemented the LAX Initiative, which was developed to address the human smuggling organizations using the Los Angeles International Airport. This operation targets not only the vulnerabilities of airline and border security, but related financial institutions and support industries directly affected by the identified criminal activity. ICE has seized approximately $1.2 million in U.S. currency, 486 undocumented aliens have been arrested, and there have been 11 Federal prosecutions in connection with these enforcement efforts.

At this time, we cannot comment on the Carreto case, since it is an ongoing criminal investigation.

BACKLOG REDUCTION PLAN

Question. CIS has reduced the benefit application backlog to 1.5 million cases, down from a high of 3.8 million cases in January of 2004. What is the plan for maintaining a 6-month average processing time—once dollars are no longer specifically set aside for this purpose?

Answer. USCIS is in the process of reengineering its business practices to ensure that it will be more efficient and effective. USCIS also plans to invest in IT transformation efforts, including a new case management system, to build the necessary infrastructure to ensure that backlogs do not return for the foreseeable future. Finally, USCIS has recently completed an in-depth staffing requirements analysis which will ensure that each USCIS office receives the appropriate amount of staff necessary to maintain the 6-month cycle time standard.

Question. What assurances do we have that the productivity gains are not coming at the expense of quality, that the right decisions are still getting made by the adjudicators?

Answer. Backlog elimination efforts will not come at the expense of national security or adjudicative integrity. USCIS has struck a solid balance in this area by ensuring that processes facilitate legal immigration, while preventing those who would misuse the system from entering or remaining in the United States. It is imperative that the integrity of the benefits process not be compromised in the effort to stimulate additional productivity.

Efforts to benchmark and assure quality are at the heart of every production initiative. For example, USCIS is committed to attacking benefit fraud and has created an Office of Fraud Detection and National Security (FDNS) specifically to lead USCIS efforts in this area. FDNS will assist USCIS adjudicators in verifying applicant and petitioner information, and will work cooperatively with ICE to ensure that fraud schemes are identified and referred to ICE for criminal investigation and prosecution. USCIS field officers have been instructed to issue Notices to Appear for removal proceedings in instances where an applicant or beneficiary has attempted to defraud the government.

CUSTOMER SERVICE

Question. In order to improve customer service, CIS is working on improving the ability of beneficiaries to interact with the Department of Homeland Security electronically. USCIS has now expanded electronic filing to support 50 percent of the total volume of benefit applications. When is the next expansion of the online filing of benefit applications planned?

Answer. The e-filing system currently includes 8 application form types, which represent approximately 50 percent of the USCIS workload. The e-filing application volume has doubled each year since its inception. The current phase entails enhancing system functionality and capabilities, which will include accepting Premium Processing filings of the Immigrant Petition for Alien Worker (Form I–140) in the third quarter of this fiscal year.

Question. Which applications does CIS plan to add next?

Answer. USCIS intends to expand e-filing, but has not yet determined which applications will be targeted for the next e-filing phase.

Question. What are the current plans for re-designing and re-launching the CIS website?

Answer. USCIS is creating a consolidated "Customer Service Portal" to integrate and align all public-facing USCIS websites. The current USCIS web configuration of "core" USCIS.gov content was completed in 1998. While the core content is continually refreshed, its underlying information architecture (IA) has never been refreshed. Moreover, three additional USCIS customer service websites, each adding a valuable new service, were appended onto USCIS.gov. However, their development was not integrated into the core website due to technical limitations at the time.

This new project will enhance the ability to manage the USCIS.gov web content; enforce the DHS branding guidelines; standardize the presentation of all USCIS.gov web content as being part of "One Voice, One Face, Many Channels," and help initiate the development of a comprehensive USCIS-wide web governance.

The development of the USCIS customer service portal will be conducted in phases. The initial phase of the project seeks to enhance USCIS.gov content by developing a comprehensive information architecture (IA) within which all current and anticipated USCIS.gov web content and e-services may be organized. The initial phase includes standing up a refreshed, customer-oriented USCIS.gov in the newly developed environment, with emphasis placed on the requirements of the USCIS Office of Communications. Additional phases will concentrate on the development of the consolidated web portal, and the requirements of other organizations providing content to USCIS.gov and integrating, to the degree possible, content from the three service-oriented websites, InfoPASS, Customer Relationship Interface System (CRIS), and e-Filing into USCIS.gov. As of March 2005, the project has been funded by the USCIS Senior Review Board. A Statement of Work for all phases of the project is currently being drafted, and USCIS anticipates awarding the contract in fiscal year 2005.

Question. What is the status of the initiative to begin electronic adjudication of Temporary Protected Status applications?

Answer. The electronic adjudication of Temporary Protected Status (TPS) applications began with the re-registration of TPS applicants from Honduras and Nicaragua on November 6, 2004, and continued with applicants from El Salvador on January 5, 2005. The next designated TPS country eligible for electronic adjudication is unknown at this point in time.

OFFICE OF FRAUD DETECTION AND NATIONAL SECURITY

Question. Please provide a detailed update on the establishment and expansion plans for the Office of Fraud Detection and National Security (FDNS).

Answer. USCIS Director Eduardo Aguirre created the Office of Fraud Detection and National Security (FDNS) to implement two high priorities that support the USCIS mission:

—Conducting effective background checks on persons seeking immigration benefits, and;

—Detecting and combating immigration benefit fraud.

Background: In fiscal year 2004, FDNS developed and implemented a joint anti-fraud strategy and initiative with the Bureau of Immigration and Customs Enforcement (ICE). To support this effort, the FDNS developed the necessary policies, procedures, and organizational structure. This included incorporating the staffs of the Service Center Fraud Detection Units (FDU) with the allocation, deployment, hiring, and training of over 150 new employees at field and headquarters locations throughout the interior United States starting in fiscal year 2004. The present staff of the FDNS is 222 permanent and term appointment employees. Of the new em-

ployees, 110 are field office Immigration Officers located within Districts, Sub-offices, Regional offices, and Headquarters. Within the FDUs and Headquarters, FDNS has 61 Intelligence Research Specialists and 30-term appointment Investigative Assistants. The remaining staff provides administrative and management support to the field officers and are located within the FDUs and Headquarters offices. Utilizing fees generated from the H–1B and L Visa Reform Act of 2004, USCIS plans to fill 160 FDNS positions. These new positions will enable FDNS to make adjustments to current staffing and provide specific levels of support for both the anti-fraud and national security operations.

Fraud

The primary objective of the anti-fraud operation is to detect and combat immigration benefit fraud by referring articulated leads to ICE for criminal investigation, and conducting administrative inquiries when ICE rejects a request for investigation. The primary duty of an FDNS Immigration Officer (IO) is to review fraud-based leads referred by adjudicators and other sources. This review consists of performing a variety of system checks, including data mining; conducting field administrative inquiries, which includes interviewing various entities; and supporting criminal investigations conducted by ICE and prosecutions by U.S. Attorneys. It also includes placing individuals in removal proceedings when fraud is verified, collecting and analyzing a variety of intelligence data, and posting look-outs on individuals involved in fraud conspiracies. By removing cases containing elements of fraud from the mainstream adjudications process, adjudicators are able to concentrate their expertise on applicants and petitioners deserving of, and eligible for, the benefits sought. Thus, this anti-fraud effort will improve the quality of adjudications, increase productivity, and reduce cycle times. The 160 new positions will enable FDNS to:

—Place FDNS IOs in the largest districts and each center, where the overwhelming majority of immigration benefit fraud exists, as well as in most of the sub-offices.

—Put a position in the Department of State's Fraud Prevention Program Office in Washington, DC, to enhance inter-departmental fraud detection and planning efforts.

National Security

Shortly after the terrorist attack of September 11, 2001, USCIS implemented a policy requiring the completion of background checks on applicants, petitioners, beneficiaries, and other individuals seeking immigration benefits. The National Security Unit has developed, and is implementing, a new policy and process pertaining to the identification, reporting, and resolution of IBIS national security hits. The Interagency Border Information System (IBIS) is the primary tool used to conduct background checks on applicants, petitioners, beneficiaries, and other individuals seeking immigration benefits. Currently, FDNS is conducting a pilot to test the electronic/paperless resolution of background checks and the entry and check of all aliases at the front end of the adjudication process.

Question. How are the relationships working with the Department of State and Immigration and Customs Enforcement?

Answer. ICE and the Department of State (DOS) have a productive working relationship and coordinate on issues of visa security as well as critical law enforcement issues often involving foreign governments. For example, ICE is working closely with DOS to develop and implement a "diplomatic" strategy to encourage several countries to accept repatriation of their citizens when they are ordered removed from the United States. Additionally, ICE works closely with DOS and other agencies as members of the Human Smuggling and Trafficking Center to synthesize intelligence, law enforcement and other information to bring effective international action against smugglers, traffickers of persons and criminals facilitating terrorists' clandestine travel. In U.S. embassies around the world, a network of ICE attachés, who with DOS, are working with their counterparts in foreign law enforcement agencies combating transnational crimes involving national security, financial, smuggling, illegal arms exports, forced child labor, child pornography, human trafficking, intellectual property rights, commercial and immigration fraud violations. ICE looks forward to continuing and expanding the collaborative relationship with DOS to further safeguard our borders and the American people.

Question. Please explain what the FDNS fraud tracking system will be? Who will have access to this system? What are the timeline and major milestones for development of the system?

Answer. FTS Requirements:

—The ability to maintain and report on fraud lead and case data in a central repository that is available at a national level to all FDNS staff and authorized external agencies
—The ability to reference benefits application data related to the subject of a case
—The ability to share case and lead data on validated fraud cases with fraud investigators at ICE
—The ability to perform reactive and ad-hoc data searches against benefits claims data
—The ability to perform data mining analysis on benefits claim data
—The ability to define fraud profiles and apply them against incoming application receipts
—The ability to track fraud profile matches and analyze data commonalities
—The ability to generate and report information for management use
—The ability to generate and automatically report G22 statistics for FDNS

Access.—FTS is being sized to accommodate up to 500 simultaneous users. This will accommodate the current 222 FDNS field staff, supervisors, managers and support staff located in geographically disparate locations nationwide, but also potential expansion. It will also accommodate information sharing with other agencies such as the FBI, CIA, Department of State, and other DHS and intelligence entities with need to access this information for national security and law enforcement purposes.

MILESTONES AND TIMELINES

	Days	Start	End
Discovery Stage	7	2/18/05	3/17/05
Design Stage	13	2/18/05	3/25/05
Configuration Stage	18	3/10/05	4/04/05
Validation Stage	15	3/22/05	4/11/05
Deployment Stage	4	4/12/05	4/15/05

Question. Please provide a detailed plan for the development and rollout of the benefit fraud assessment tool, including timelines and milestones.

Answer. U.S. Citizenship and Immigration Service's (CIS) Fraud Detection and National Security (FDNS) Unit will implement a Benefit Fraud Assessment program (BFA). This program was approved in February 2005, and will be implemented in various phases through October 2005. ICE supports FDNS conducting the BFA so that ICE can direct its resources to investigating/prosecuting actual benefit fraud violators.

OFFICE OF CITIZENSHIP

Question. Please provide the following information regarding the Guide for New Immigrants: which languages will the guide be produced in; how many will be printed in each language in the initial run; how will the guides be distributed electronically and physically; what is the timeline for translating the guide into each of the planned languages; and what is the timeline for producing hard copies in each language.

Answer. To ensure that immigrants from a variety of language groups have access to the Guide, the Office of Citizenship will translate the English version of the Guide into ten (10) languages—Spanish, Chinese, Vietnamese, Tagalog, Portuguese, Russian, French, Korean, Haitian Creole, and Arabic.

Hard copies of the Spanish and English versions of the Guide will be available for purchase through the Government Printing Office (GPO), and all other versions will be accessible online. In order to initially market the product, the Office plans to print approximately 250,000 copies of the English guide and 150,000 copies of the Spanish guide.

In addition of the current availability of the English Guide online (additional languages to be posted as translations are completed) the Office is coordinating a national mailing list of community and faith-based organizations, immigration service providers, State and local contacts and adult educators in an effort to disseminate the Guide nationally. USCIS Community Liaison Officers and local field Directors will also receive copies of the Guide for additional local dissemination. GPO order forms will also be included as part of the dissemination effort. In addition to planned dissemination efforts, the Office also plans to implement a comprehensive outreach/public education effort in key communities. These events will be strategically located according to where the centers of the various foreign language communities are. Plans include high-profile events in: Los Angeles for the Spanish version

(May); San Francisco for the Chinese, Tagalog, and Vietnamese versions (May); New York City for the Russian and Korean versions (July); and Detroit/Dearborn for the Arabic version (August).

Spanish translation should be completed in April; Chinese, Tagalog and Vietnamese will be completed in May; Russian, Korean and Arabic will be completed in June; and Portuguese, Haitian Creole and French will be completed in July.

Hard copies of the English and Spanish guides will be available in June. All other translation will be available online late summer. There are currently no plans to print hard copies of the additional languages.

STAFFING

Question. Please provide a complete FTE staffing plan for fiscal year 2005 and 2006, including but not limited to; location (i.e., District Office, Service Processing Center, etc), position type (i.e., Immigration Information Officer, Adjudicator, etc), and physical location (i.e., Burlington, VT; Dallas, TX; etc).

Answer. Please see tables provided below.

USCIS FTE Staffing Plan

Region	District	Current On-Board		
		Adjudicators (NFC)[1]		All Other USCIS Staff
		Perm	Term	Total
EASTERN	Atlanta	23	28	**62**
	Baltimore	17	13	**39**
	Boston	45	11	**84**
	Buffalo	11	3	**38**
	Cleveland	11	6	**32**
	Detroit	20	10	**32**
	Miami	133	20	**146**
	Newark	59	13	**71**
	New Orleans	16	12	**43**
	New York District	157	52	**219**
	Philadelphia	18	13	**44**
	Portland	4	-	**16**
	San Juan District	9	4	**29**
	Washington, D.C.	22	9	**43**
CENTRAL	Chicago	62	42	**98**
	Dallas	34	22	**53**
	Denver	14	16	**28**
	EL Paso	11	9	**32**
	Helena	4	2	**14**
	Harlington	10	14	**26**
	Houston	43	42	**56**
	Kansas	12	6	**23**
	Omaha	8	3	**15**
	San Antonio	14	21	**39**
	St. Paul	10	7	**19**
WESTERN	Anchorage	3	1	**6**
	Hawaii	11	-	**28**
	Los Angeles	205	109	**381**
	Phoenix	34	23	**56**
	Portland	9	6	**22**
	Seattle	23	14	**44**
	San Francisco	127	39	**138**
	San Diego	27	17	**49**
SERVICE CENTERS	California	162	157	**325**
	Nebraska	136	153	**230**
	Texas	131	94	**211**
	Vermont	216	185	**293**
NBC	Missouri	-	90	**64**

USCIS FTE Staffing Plan

		Workload Staffing Requirements										
Region	District	Avg 04-06 Required Adjudicator Staffing Level (IMAPS)[1]		Supervisory Adjudicators: Imposed Position Counts[2]		Section Managers: Imposed Position Counts[3]		Leadership[4]	Clerks: Imposed Position Counts[5]		FDNS	ASC Managers
		FY '07 Perm	'05-'06 Term	FY '07 Perm	'05-'06 Term	FY '07 Perm	'05-'06 Term	Authorized	FY '07 Perm	'05-'06 Term	Authorized	Authorized
EASTERN	Atlanta	54	28	8	4	2	-	4	18	10	3	4
	Baltimore	33	6	5	1	2	-	1	10	2	1	3
	Boston	66	12	*8*	*2*	2	-	5	21	6	3	4
	Buffalo	12	1	2	1	-	-	2	5	1	2	3
	Cleveland	18	7	*2*	*2*	-	-	3	7	3	1	3
	Detroit	24	3	3	1	-	-	1	8	1	2	2
	Miami	145	52	20	9	3	-	6	46	17	7	8
	Newark	74	12	10	3	3	-	3	23	4	4	3
	New Orleans	24	6	4	2	-	-	4	8	2	2	6
	New York District	175	106	22	14	6	4	2	52	32	7	9
	Philadelphia	32	8	5	*1*	-	-	2	10	4	1	4
	Portland	4	2	*1*	-	-	-	2	2	2	-	1
	San Juan District	6	1	1	1	-	-	2	2	1	1	1
	Washington, D.C.	38	13	5	2	-	-	3	13	5	2	2
CENTRAL	Chicago	74	22	10	5	2	-	4	24	8	4	9
	Dallas	39	12	6	3	2	-	3	12	4	2	4
	Denver	23	4	3	2	-	-	2	8	2	1	4
	EL Paso	13	2	2	1	-	-	2	4	2	1	3
	Helena	4	2	-	-	-	-	2	2	2	-	3
	Harlington	9	4	2	1	-	-	1	3	2	1	2
	Houston	39	9	5	2	2	-	2	12	3	3	2
	Kansas	16	1	3	1	-	-	2	5	1	1	3
	Omaha	8	1	1	1	-	-	2	3	1	1	2
	San Antonio	22	-	3	-	-	-	1	7	-	2	1
	St. Paul	18	3	3	1	-	-	1	6	1	1	3
WESTERN	Anchorage	3	1	1	-	-	-	1	1	1	-	1
	Hawaii	11	5	1	1	-	-	2	4	3	1	2
	Los Angeles	195	38	25	5	7	2	5	58	12	11	13
	Phoenix	36	15	6	*2*	-	-	5	12	7	3	4
	Portland	11	1	2	1	-	-	1	4	1	1	1
	Seattle	29	3	*3*	1	-	-	3	9	2	2	4
	San Francisco	114	18	16	4	2	-	5	35	7	7	10
	San Diego	28	4	4	1	-	-	1	9	2	3	2
SERVICE CENTERS	California	204	126	26	16	7	4	2	61	38	18	
	Nebraska	200	81	25	11	7	3	2	60	25	21	
	Texas	201	97	26	13	7	4	2	60	29	20	
	Vermont	200	92	25	12	7	3	2	60	28	33	
NBC	Missouri	121	10	16	2	4	-	2	37	3	13	

USCIS FTE Staffing Plan

Region	District	Staffing Distribution[5]							
		IIOs	Analysts	Admin	Records	Customer Service	Computer Info Service	FTE Surplus	Total USCIS Staff
EASTERN	Atlanta	31	4	6	18	1	-	-	195
	Baltimore	12	2	3	8	1	-	-	90
	Boston	28	4	5	17	1	-	-	184
	Buffalo	6	-	-	3	-	-	-	38
	Cleveland	12	-	2	7	-	-	-	67
	Detroit	9	2	2	5	-	-	-	63
	Miami	60	9	14	34	2	1	-	433
	Newark	21	4	6	15	1	1	-	187
	New Orleans	11	-	-	9	-	-	-	78
	New York District	67	13	20	34	4	3	-	570
	Philadelphia	13	2	2	8	1	-	-	93
	Portland	2	-	-	1	-	-	-	17
	San Juan District	3	-	-	2	-	-	-	21
	Washington, D.C.	16	2	3	10	1	-	-	115
CENTRAL	Chicago	26	4	6	12	1	1	-	212
	Dallas	16	3	3	11	1	-	-	121
	Denver	10	1	1	6	-	-	-	67
	EL Paso	6	-	-	4	-	-	-	40
	Helena	3	-	-	1	-	-	-	19
	Harlington	5	-	-	4	-	-	-	34
	Houston	16	3	4	7	1	1	-	111
	Kansas	6	-	-	5	-	-	-	44
	Omaha	3	-	-	2	-	-	-	25
	San Antonio	7	1	1	4	-	-	-	49
	St. Paul	8	1	2	5	-	-	-	53
WESTERN	Anchorage	2	-	-	1	-	-	-	12
	Hawaii	6	-	-	4	-	-	-	40
	Los Angeles	55	11	17	59	4	2	-	519
	Phoenix	20	2	4	12	-	-	-	128
	Portland	5	-	1	3	-	-	-	32
	Seattle	14	1	2	8	-	-	-	81
	San Francisco	38	7	10	28	1	1	-	303
	San Diego	10	2	2	6	1	-	-	75
SERVICE CENTERS	California	42	28	37	24	14	19	21	687
	Nebraska	36	24	31	21	12	16	20	595
	Texas	38	26	33	22	13	17	20	628
	Vermont	37	25	32	21	13	17	20	627
NBC	Missouri	33	11	15	10	6	7	12	302

[1] Based on Sep '04 IMAPS; adjudicator requirements rounded up; excludes contractors.

[2] Ratio = 8:1 Supervisory Adjudicator positions include: SDAO and SCAO.

[3] Ratio = 4:1, 7:2, 12:3 and 17:4. Positions also include: Section Chief, and ACD.

[4] Positions include: DD, DDD, SCD, DSCD, and OIC.

[5] Ratio = 3:1 Based on the ratio of current on-board Adjudicator Clerks to Adjudicators. "Other" designation excluded.

[6] Staffing distribution calculations are based on Avg 04-06 Adjudicator staffing requirements.

[7] Total On-Board figures include both Perm and Term designations. Supervisory Adjudicators include all management-level adjudicator positions.

Question. Please provide a breakout of attrition rates for each of fiscal years 2003, 2004, and 2005 by type of position and location.

Answer. USCIS only has attrition rates for fiscal year 2004. For the major position types, they are:

—Adjudications Officer: 2.3 percent
—Asylum Officer: 6.1 percent
—Asylum/Adjudications Clerk: 2.3 percent
—Immigration Information Officer/Customer Service Representative: 1.2 percent

Data is not available by location.

Question. Please provide a chart with the numbers and types of employees that have been trained at Glynco, GA for each of fiscal years 2003, 2004, and 2005.

Answer:

Position type	Fiscal year 2004	Fiscal year 2005 (estimate)
Adjudication Officer	751	1,098

Position type	Fiscal year 2004	Fiscal year 2005 (estimate)
Asylum Officer	116	170
Immigration Information Officer	142	207
Other	58	85
Total	1,067	1,560

Fiscal year 2003 data is not available.

CALL CENTERS

Question. Please provide a chart with the number of contractors assigned to each call center for fiscal years 2004 and 2005.

Answer. USCIS does not determine the number of contractors assigned to each contract call center. Under our contract, the vendor is required to have sufficiently trained staff to meet our performance requirements, and is responsible for determining the placement and size of each of its operations.

Question. Please provide a chart for each of fiscal years 2004 and 2005 of the total number of calls received by call center, broken out by type of call.

Answer. USCIS has two kinds of call centers. Contract call centers, which provide initial live assistance, and USCIS staffed call centers, which answer questions that cannot be answered by the contract staff.

Our contract call centers operate as one. We do not route calls to our general customer service line based on the nature of the call, but based on agent availability. Calls are routed to the next available agent with the appropriate language skills regardless of location. Thus, staff scheduling, availability and performance affect call routing, not the nature of the call. USCIS, therefore, does not track information by type of call.

The table below shows the volumes and percentage of live assistance calls handled by staff at each of the four (4) contract call centers for fiscal year 2004 and fiscal year 2005 (through mid-March).

	2004		2005 (through mid-March)	
	Volume	Percent	Volume	Percent
Phoenix, Arizona	1,269,059	16.0	531,867	17.1
Lawrence, Kansas	1,534,164	19.3	636,945	20.4
Corbin, Kentucky	4,800,717	60.5	1,809,688	58.1
Arlington, Virginia	334,911	4.2	138,153	4.4
Total live assistance calls handled by contract call centers	7,938,851		3,116,653	
Total calls received to USCIS	21,295,256		8,454,022	
Percent of total calls that were handled by contract call centers		37.3		36.9

QUESTIONS SUBMITTED BY SENATOR TED STEVENS

ICE—CYBER CRIME CENTER

Question. Last year, $4.2 million was secured in the fiscal year 2005 Homeland Security Appropriations Act to expand the ICE Cyber Crime Center to ICE field offices. Are these funds at risk of being diverted to address the base budget shortfall within ICE this fiscal year?

Answer. At this time, it is ICE's intent to execute the entire $4.2 million in fiscal year 2005 for the purpose for which it was appropriated.

IMMIGRATION SERVICES

Question. With the split of immigration and enforcement functions precipitated by the creation of the Department of Homeland Security, Alaska's capitol, Juneau, was left with no personnel to provide immigration services. Without immigration services, immigrants are forced to fly to Anchorage to access services. What steps have been taken by the Homeland Security Department to ensure Juneau's need for immigration services will be met?

Answer. Since the creation of USCIS, the agency has met the needs of Juneau and other distant communities of Alaska by sending an officer 2 or 3 times each year on periodic circuit rides to conduct benefits interviews, naturalization cere-

monies, and community outreach. USCIS has recently expanded the circuit rides to 4 times a year, even though there were only 400 Naturalization and Adjustment of Status cases in the entire District in the first quarter of this year. The most recent trip was in November 2004, and there are trips to Juneau scheduled for April, August, and October of 2005. The current cycle times are just over 6 months for naturalization, and just under 6 months in Adjustment of Status cases.

QUESTIONS SUBMITTED BY SENATOR PETE V. DOMENICI

LAND PORT OF ENTRY

Question. America has 197 land ports of entry, and it has been almost 20 years since we launched a major effort to upgrade infrastructure at those ports. That last effort occurred in 1986—almost 15 years prior September 11, 2001.

Since September 11, we have placed increasing emphasis on upgrading protective measures for our airports, seaports, and critical infrastructure. It is imperative that we also improve land port security if we are going to be successful in the war on terror. To that end, I intend to introduce a bill which will authorize additional funds for investment in our Nation's border crossings.

Have you considered what kinds of improvements are necessary at our land ports of entry and how much these upgrades might cost?

Answer. CBP has initiated a Construction Master Planning Process that will allow for increased security at the Nation's borders by providing critical facility and infrastructure improvements that are prioritized using a rigorous capital investment planning process.

The planning methodology and resulting allocation of construction projects will optimize available resources to support the expanded methods of CBP operations and comprehensive border enforcement strategy. The construction planning process aligns with the DHS mission and strategy, forecasted future growth, identify and justify required projects and estimate their associated costs. The CBP Construction Master Planning Process was developed in response to the reporting requirements included in House Report 108–774 and House Report 108–541.

Question. Based on your experience at CBP, what do you believe are the three top priorities for securing our land ports?

Answer. Since September 11, 2001, CBP has tightened procedures for entry into the United States at all ports of entry, based on three strategic priorities:

—*Advance Information and Risk-Targeting.*—CBP has moved forward with programs that provide information regarding cargo and passengers as far in advance of arrival to the United States as possible, and systems to review this information and develop targeted response to high-risk cargo and individuals. These programs and systems include C–TPAT, CSI, advance cargo manifests, Advance Passenger Information Systems, all screened through our National Targeting Center.

—*State of the Art Technology.*—CBP is investing in state-of-the-art technology, including non-intrusive radiation detection systems, making additional information systems available to inspectors at the ports of entry, and addition of biometric and other systems to enhance security.

—*Training.*—CBP has significantly revised and reprioritized our training for CBP Officers based on operational priorities, beginning with the establishment of anti-terrorism protocols for all ports of entry and developing and implementing anti-terrorism training for all CBP Officers.

Question. Specific improvements are needed at the Columbus port of entry in New Mexico, and I understand that the General Services Administration (GSA) has proposed that construction on the Columbus project begin in 2007 or 2008. Do you support GSA's recommendation and will you keep the project on track for construction?

Answer. CBP has requested GSA to modernize and expand the border station in Columbus, NM. The existing facility constructed in 1987, is a full service port of entry with pedestrian, non-commercial and commercial traffic. It is the only 24-hour border crossing point for pedestrians and privately owned vehicles in New Mexico. The facility is in need of significant renovation and expansion to safely process the increased volume of traffic that has occurred since originally constructed.

CBP has requested GSA to include this project at the earliest opportunity. If approved for design in fiscal year 2007, construction should begin in fiscal year 2009.

QUESTIONS SUBMITTED BY SENATOR RICHARD C. SHELBY

OPERATION PREDATOR

Question. Mr. Secretary, first, let me thank you again this year for ICE's efforts to stop the exploitation of children. I understand that Operation Predator has had many successes and I am glad to hear of its achievements. I believe it is a critical program and I hope it continues to be successful. We should continue to do all within our power to ensure that children around the world are protected from those individuals that would harm them and shamelessly exploit them for simple pleasure and monetary gain.

To that end, I ask that you share with the Committee some of ICE's other efforts to eliminate the abuse and exploitation of children. I know that you have many partners in this effort. I would appreciate you expounding on your opening statement as to what ICE is doing and who you are working with to accomplish these goals.

Answer. In addition to Operation Predator, ICE attempts to eliminate the abuse and exploitation of children by enforcing the laws related to Forced Child Labor (FCL). ICE has implemented a proactive outreach schedule targeting an audience comprised of leaders in domestic industry and their employees/agents responsible for foreign purchases and related internal security procedures. Our goal is to educate this community, promote voluntary compliance, and encourage vigilance and reporting of suspected violators. The ICE FCL program staff regularly attends other United States Government agency, foreign government, and non-governmental organization functions related to forced or indentured child labor. In particular, FCL program staff attends and participates in monthly meetings with the National Child Labor Coalition, an organization that exists to serve as a national network for the exchange of information regarding children in an effort to end child labor exploitation by promoting progressive initiatives and legislation; established contacts with various domestic industry trade show representatives and coordinated participation in commodity specific events; and published the Forced Child Labor Advisory and accompanying pamphlet, produced in English and translated into 5 foreign languages for distribution in training and outreach activities. ICE currently has 20 open investigations related to allegations of the importation of products manufactured or produced with forced or indentured child labor. During fiscal year 2005, three new investigations were opened, twelve were closed, and one investigation is in pending status.

During 2004, ICE hosted two international symposiums on FCL and related child exploitation issues as defined in the International Labor Organization (ILO) Convention 182. These symposiums hosted in Singapore and Johannesburg, South Africa, were geared at educating foreign law enforcement partners on U.S. laws, promoting information sharing, and enhancing networking vital to successful investigations, and included presentations and training on: Forced Child Labor, the Protect Act and Operation Predator, Child Pornography, Basic Computer Forensics and Investigative Techniques, and Child Sex Tourism. In addition, at the Johannesburg, South Africa conference, a block of training was conducted by ICE on human smuggling and trafficking particularly with regard to children on the African continent.

In regard to human smuggling and trafficking into the United States, ICE does not keep statistics delineating children versus adults. However, in terms of all human trafficking (men, women, and children), many of these victims are lured from their homes with false promises of well-paying jobs; instead, they are forced or coerced into prostitution, domestic servitude, or other types of forced labor. ICE, with its wide range of authorities, expertise and capabilities attacks human trafficking organizations through the aggressive use of human trafficking, smuggling and money laundering statutes, as well as identification and seizure of criminal proceeds and assets. Each and every allegation received by the ICE FCL program is researched, analyzed, and referred to the appropriate domestic or foreign office for further investigation. ICE's education and outreach process provides guidance to ICE agents in distinguishing the clear differences between human smuggling violations and human trafficking. This process has enabled ICE agents, our State and local law enforcement partners and community groups to better understand and identify trafficking violations and to better care for victims. ICE office of investigations has also conducted extensive outreach and training with our law enforcement partners abroad. Coordinating with the ICE Attachés in numerous countries, ICE works to combat trafficking organizations, in source and transit nations, as well as in the United States.

ILLEGAL IMMIGRANTS

Question. Among each of your roles, is the charge to secure our borders and to control illegal immigration. Estimates of the number of illegal immigrants range greatly. Some say 8 million others say millions more. I believe that we all know that 8 million is an extremely conservative estimate.

What is your best estimate on the number of illegal aliens currently residing in the country?

Answer. It is estimated that the number of illegal aliens currently residing in the country is most likely between 11–12 million.

Question. How many new illegal aliens entered the country last year?

Answer. The total for "first time" illegal aliens, in fiscal year 2004, making entry into the United States between the ports of entry is 608,073. These numbers are derived from using the data provided in the Enforce Integrated Database (EID). This data is based on persons identified by biometric data (fingerprints) as first time apprehensions.

Question. Is that an increase or a decrease from the previous year?

Answer. There was a 20 percent increase in first-time apprehensions/entries into to the United States in fiscal year 2004 compared to fiscal year 2003.

Fiscal year 2004—608,073.

Fiscal year 2003—504,889.

Question. If we are so uncertain about the numbers, doesn't that seem to indicate that we are not doing enough to secure our borders and our homeland?

Answer. U.S. Customs and Border Protection is enhancing and planning operations in areas along the borders which pose the greatest threat to national security. With the development and implementation of the Border Patrol's National Strategy, a measured but aggressive approach is being taken to increase border security. The guidelines and goals outlined in the National Strategy have been translated into the CBP/USBP implementation plan.

VISA OVERSTAYS

Question. Another major problem with our immigration system is the fact that many of those people currently counted as illegals actually entered the country legally, but have overstayed their visas.

Does the Department have any recent numbers on visa overstays?

Answer. The US-VISIT Program Office conducted an analysis of biometric entry and exit data for the first 9 months of the program (January 5, 2004 to September 30, 2004) and initially, the findings indicate that, for visa holders on whom biometrics are collected at both entry and exit, nearly 90 percent exit the country before their periods of admission expire. In addition, US-VISIT's preliminary findings show that there is no exit record for less than 1 percent of these visa holders. Due to current limitations in capabilities to capture complete entry and exit data on all visa holders, the small sample size, and the abbreviated period covered by the analysis, US-VISIT is unable to provide more detailed findings.

Question. How many temporary visa holders never return to their home country?

Answer. Except for the preliminary information mentioned in the previous question, US-VISIT does not yet contain all the technological elements that would readily provide this type of status information. However, according to a report from the Office Immigration Statistics using data from the Nonimmigrant Information System (NIIS), a total of 23.6 million nonimmigrant departures were recorded by NIIS during 2003. Of those, 22.1 million or 94 percent were matched to an arrival and showed valid arrival and departure dates.

The proportion of all admissions matched varies among the broad categories of admission. Short-term visitors had the highest match rate (95 percent), followed by diplomats and other representatives (93 percent), students and temporary workers (88 percent), and expected long-term residents (87 percent). Records missing the category of admission have the highest non-match rate (48 percent) but as a group represented less than one percent.

The report also gives length of visit estimates. Nonimmigrants included in NIIS who departed in 2003, remained in the United States an average, or mean, of 34 days, or just under 5 weeks, per visit. The median length of visit was 8 days, indicating half of all departing nonimmigrants remained in the country for 8 days or less. Over 95 percent of departing nonimmigrants remained for less than 6 months per trip, with approximately 4 percent remaining between 6 months and 1 year, and 1 percent remaining 1 year or more.

Question. Can you tell us what percentage of the total illegal population is visa overstays?

Answer. It is very difficult to accurately estimate either population. The fiscal year 2006 US-VISIT budget request includes $24 million for the person-centric view that would begin the transformation of these systems so as to provide timely and accurate visibility to all DOS and DHS officers associated with the visa process regarding those who chronically overstay, or are overstaying for extended periods.

Question. Given that these people make up a large percentage of our illegal population, has any consideration been given to strengthening the vetting process? What I mean by that is, if a large percentage of those people obtaining visas are not returning do you think there a breakdown somewhere in the process?

Answer. Managing the entry, stay and departure of alien visitors is a major component of controlling our borders and requires collecting information regarding the movement of aliens in, through, and out of the United States. The information in the US-VISIT system is available to Customs and Border Protection (CBP) officers at ports of entry, special agents in Immigration and Customs Enforcement (ICE), adjudications staff at U.S. Citizenship and Immigration Services (CIS) services offices, U.S. consular offices, and other law enforcement agencies. Such information allows these officers to identify and take action against those who violate the law, to locate individual aliens of interest to law enforcement entities, to validate the immigration status of aliens so that only eligible persons receive immigration benefits, and to intercept terrorists and other persons who should not be allowed into the country. Additionally, the United States Government (USG) will be able to use this data to make informed policy and management decisions regarding enforcement prioritization, participation in visa waiver programs, or immigration benefit programs.

Collecting exit information through US-VISIT will strengthen the vetting process by giving officials who issue visas timely, accurate and comprehensive visibility into an applicant's compliance patterns, so that appropriate action can be taken on the visa request. Once all of the elements of the exit/entry system are in place (i.e., at all land, air and sea points of entry, including immigration status information capabilities), we will have the ability to accurately assess and investigate the overstay population.

Question. Following-up on that what is your agency doing now and what are you planning to do in the future to ensure that this does not continue to be a problem?

Answer. The Homeland Security Act of 2002 gave DHS the responsibility for several significant national security programs/initiatives to track nonimmigrant aliens' compliance with the terms and conditions of their admission to the United States. These programs/initiatives include: the Student and Exchange Visitor Information System (SEVIS), the National Security Entry/Exit Registration System (NSEERS), and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. ICE formed the Compliance Enforcement Unit in June 2003, to investigate criminal and administrative violations identified through these programs. The CEU receives violator data from these programs/initiatives, analyzes the data and sends proactive investigation requests to field offices to locate and remove the violators. The CEU will continue to exploit the benefits of these programs/initiatives.

Additionally, the fiscal year 2005 budget provides for the hiring of additional ICE criminal investigator positions to be assigned to compliance enforcement units across the country. ICE plans to staff these additional positions in field offices to support compliance enforcement investigations generated by the ICE Headquarters CEU. The positions will support compliance enforcement of the US-VISIT, NSEERS, and SEVIS programs based on current enforcement need projections.

Question. I know that US-VISIT is slowly being implemented.

What progress has been made to date and what assurances can you give us that we know who is legally entering the United States?

Answer. The Department of Homeland Security has met the December 31, 2003, and December 31, 2004, Congressional deadlines to deploy an entry-exit program that strengthens security and facilitates travel for legitimate visitors while protecting their privacy and ensuring the integrity of our immigration system. In conjunction with the Department of State's Biometric Visa Program, we are creating a continuum of security measures that begins before individuals enter the United States and continues through their arrival and departure from the country. US-VISIT also works with commercial carriers to receive notification of passenger lists before passengers arrive in and depart from the United States.

Since its beginning on January 5, 2004, US-VISIT has implemented entry procedures at 115 airports, 14 seaports, and in the secondary inspection areas of the 50 busiest land ports of entry. In September 2004, US-VISIT was expanded from individuals with visas to include processing of visitors traveling to the United States under the Visa Waiver program. US-VISIT processed over 20 million foreign trav-

elers from January 5, 2004, to February 24, 2005, and has prevented 536 criminals and immigration violators, including Federal and State prison escapees, from gaining admission to the United States.

US-VISIT is protecting our visitors by making it virtually impossible for anyone else to claim their identity should their travel documents to be stolen or duplicated. Our fingerprint matching system has an accuracy rate (True Acceptance Rate or TAR) of 99.6 percent for one-to-one verification and a TAR of 96 percent for one-to-many identification. DHS is currently working with National Institute of Standards and Technology and industry leaders on several initiatives to examine mechanisms to increase the level of accuracy.

Later this summer, US-VISIT will conduct tests using automatic identification (Radio Frequency Identification Technology or RFID) at land ports of entry to capture entry/exit information. US-VISIT is on track to deploy entry procedures to the remaining land ports of entry by December 31, 2005, meeting the Data Management Improvement Act (DMIA) mandate.

The work of US-VISIT will extend far past these current efforts. In the Intelligence Reform and Terrorism Prevention Act of 2004, Congress included requirements and actions to be taken by DHS, the Department of State and US-VISIT with the goal of completing a biometric entry and exit data system as expeditiously as possible. US-VISIT is preparing a Strategic Plan that will describe how a single, unified approach to immigration and border management—a U.S. Immigration and Border Management Enterprise—will look and operate in the future. The Plan will include the overarching vision for how the United States Government will manage immigration and its borders, as well as how data, facilities, and information technology will contribute to the Enterprise mission.

Question. Conversely, I believe it is important that we know who is leaving the country. Specifically, that ties directly into the visa overstays. If we know that people are leaving we will have a very good accounting of the number of folks that have chosen to stay here illegally. Can you tell us what progress has been made on implementing the exit portion of the program?

Answer. In the air and sea environments, DHS is currently collecting biographic arrival and departure data through electronic manifests submitted by the transportation carriers and is using this data to identify alien travelers whose authorized periods of admission have expired and for whom no matching departure information is available. This information is already being shared with U.S. Immigration and Customs Enforcement (ICE). US-VISIT is working collaboratively with the ICE Compliance Enforcement Unit (CEU) to research existing data limitations and develop protocols and procedures to effectively vet these records through additional data sources to develop more complete, accurate and actionable information. Additionally, US-VISIT is conducting pilots to determine the most effective means of capturing exit information.

Airport and Seaport Pilots.—US-VISIT is currently piloting three alternative methods of biometric departure confirmation at one seaport (Miami International Cruise line Terminal) and eight airports (Chicago O'Hare; Baltimore Washington International; Denver International; Dallas/Fort Worth International; Newark Liberty International; Luis Munoz International in San Juan, Puerto Rico; San Francisco International; and Detroit Metropolitan Wayne County). DHS anticipates making a decision on the best method(s) to implement shortly, and determining a schedule to expand biometric exit.

Automated Land Border Entry-Exit.—Later this spring, US-VISIT will begin testing Radio Frequency Identification (RFID) technology. Using an automatic identifier, RFID technology can detect a visitor at a distance and provide primary inspection with entry information as well as provide a mechanism for an accurate and timely record of exits. By July 31, 2005, testing will begin at the ports of Nogales East and Nogales West in Arizona, Alexandria Bay in New York, and the Pacific Highway and Peace Arch in Washington. Testing will continue through the spring of 2006.

Question. When does the Department expect the entire program to be fully operational?

Answer. DHS will complete deployment of an initial biometric-based entry and exit program at all U.S. ports of entry by the end of 2005, meeting the requirements established by legislation. It is important to note that the Data Management Improvement Act, which established the majority of initial deadlines, only required the integrating of existing arrival and departure information—it did not require the collection of new information, such as biometrics. The Enhanced Border Security and Visa Entry Reform Act contained a requirement to biometrically compare and authenticate certain travel documents by established dates. DHS, recognizing the importance of biometrics in the process, added the requirement to collect biometric in-

formation, and is establishing additional procedures, beyond those required by statute, to enhance security.

Ultimately, US-VISIT will manage data on foreign nationals covering their interactions with U.S. officials before they enter, when they enter, while they are in the United States, and when they exit. This comprehensive view of immigration and border management will create a virtual border and will improve interactions with foreign nationals. In its strategic plan (required under the Intelligence Reform and Terrorism Prevention Act of 2004) US-VISIT will describe how the U.S. Immigration and Border Management Enterprise will look and operate in the future.

Question. Mr. Secretary, can you tell me how many people were detained or deported for overstaying their visas last year? Does ICE take proactive measures towards apprehending overstays?

Answer. Statistics obtained from ICE's administrative booking system, ENFORCE, revealed that in fiscal year 2004, 3,784 nonimmigrants were processed for removal from the United States under the charge of INA 237(a)(1)(C)(i), violation of nonimmigrant status or condition of entry. The INA does not have a specific charge for visa overstays. The above number will include individuals that violated their nonimmigrant status by overstaying their visa, as well as other nonimmigrant violators. These other nonimmigrant violators include: student visa violators, individuals found working without authorization, and nonimmigrants that have violated their status by committing a crime.

The Compliance Enforcement Unit (CEU) receives violator data from NSEERS, US-VISIT, and SEVIS. The CEU analyzes the data and sends proactive investigation requests to field offices to locate and remove the violators. In fiscal year 2004, the CEU sent out over 2,050 visa overstay leads generated by NSEERS, US-VISIT, and SEVIS to ICE SAC offices throughout the country. The CEU will continue to receive and assign overstay leads to ICE SAC offices for investigation.

Question. What are the ramifications and penalties for overstaying a visa? There must be a way to keep track of these folks.

Answer. A nonimmigrant that has failed to maintain the status in which he/she was admitted, or fails to comply with the conditions of any such status, to include nonimmigrants that stay beyond their period of admission, is subject to removal from the United States under the charge of INA 237(a)(1)(C)(i), violation of nonimmigrant status or condition of entry.

DHS implemented the US-VISIT program in January 2004, to address a Congressional mandate to implement a nationwide entry-exit tracking system. Once fully implemented, US-VISIT will biometrically document the entry and exit of all foreign visitors to the United States. The CEU works closely with the US-VISIT Program to identify potential visa overstay violators and to conduct the necessary follow up investigations.

BORDER SECURITY

Question. Every year, I travel to every county in Alabama to hear the issues of my constituents and one of their greatest and most frequent concerns is immigration and more to the point illegal immigration. Every year I feel compelled to tell my constituents that while we are making progress we are nowhere near where we need to be.

What is the Directorate doing to make our borders more secure and to eliminate the influx of illegal aliens?

Answer. ICE is a key player—along with our partners at U.S. Customs and Border Protection (CBP) and U.S. Citizenship and Immigration Services (USCIS)—in the Department's mission to secure the borders and restore integrity to the Nation's immigration system. That is a mission ICE takes very seriously—as the tragic results that can follow when those wishing to do us harm breach the Nation's border security and exploit immigration laws. The key to this effort is prioritization—systematically attacking the most serious threats first. Specifically, ICE has made the apprehension and removal of dangerous criminal aliens and national security threats our top enforcement priority. This is not to suggest that ICE does not fully and consistently enforce the law in other situations but that ICE focuses on addressing the serious threats that individuals with possible terrorist associations, fugitive alien absconders, violent criminal aliens, sexual predators, and others pose to our communities, our families, and our Nation. ICE's objective is to strategically target our resources and authorities on the most dangerous aliens in order to remove them from the streets before they can do harm.

It's a strategy that is getting results. In fiscal year 2004, ICE removed more than 160,200 aliens with more than half of them having prior criminal convictions and 18 fugitive absconder teams across the Nation who apprehended more than 11,000

fugitives last year. ICE created a "Most Wanted" list of the most dangerous criminal aliens, which has been a valuable tool for generating tips and leads. From the original list, nine of the ten were captured within a few weeks, and the tenth was determined to have already left the country. Under ICE's "Operation Predator," which targets pedophiles, child sex tourists, and child pornographers we have arrested more than 5,000 child sex predators who exploit children for pleasure or profit. Approximately 40 percent of the predators arrested under this program have been illegal aliens, and an additional 20 percent have been visitors to the United States who were "out of status," meaning that they had overstayed or otherwise violated the terms of their admission.

Another priority is to dismantle criminal organizations that smuggle and traffic human beings for profit. In fiscal year 2004, ICE arrested more than 1,630 human smugglers. Operation ICE Storm, an initiative launched in 2003 to target violent human smuggling networks in Arizona, has brought charges against more than 300 defendants and resulted in the seizure of more than $7 million. This unprecedented seizure of alien smuggling proceeds is a direct result of the combination of ICE's immigration and customs authorities (particularly customs expertise in financial crime investigation). Law enforcement authorities in Arizona have credited Operation ICE Storm with a dramatic decrease in alien-related kidnappings and other violent crime in the Phoenix metropolitan area.

ICE's Law Enforcement Support Center (LESC) responded to more than 603,000 immigration status inquiries from Federal, State, and local authorities in fiscal year 2004 and placed more than 15,000 immigration detainers with police agencies nationwide allowing ICE to more efficiently remove aliens from the United States once their jail term has expired. ICE is also fostering innovative new relationships through our 287(g) program, which delegates authority for immigration enforcement to State and local law enforcement. Under the terms of Section 287(g) of the Immigration and Nationality Act (Illegal Immigration Reform and Immigrant Responsibility Act, Sec. 113, April 30, 1996), State and local authorities can request this authority for their jurisdictions. Once this agreement is in place, ICE provides officers with a 5-week training program in immigration issues, and provides supervision and support for State and local officers engaged in immigration enforcement. These authorities are currently in effect in Florida and Alabama.

The examples above are just a sampling of the critical immigration enforcement accomplishments of ICE. By aggressively enforcing our immigration laws and targeting criminals, ICE seeks to deter criminal and terrorist organizations that threaten our way of life. ICE will continue to work with its partners at the Federal, State, and local levels to secure the borders and protect the homeland.

Question. How many aliens have been detained and deported in the last year?

Answer. Based on data reported in the Deportable Alien Control System (DACS), as of January 2005, ICE removed/deported 161,090 aliens in fiscal year 2004. This number of final order removals is made up of criminals and non-criminals, detained and non-detained aliens. This does not include any voluntary removals, nor does it include any expedited removals, largely handled by the bureau of Customs and Border Protection. Virtually all of these removals were detained at least 1 day prior to their removal.

Based on data reported in DACS, as of January 2005, 235,449 aliens were detained at some point during fiscal year 2004. Some of these aliens were detained and then released to the community (bond, supervision, recognizance, etc). Others were granted voluntary departure, or transferred to other law enforcement agencies. Finally, some are still in detention for various reasons.

Question. If a Mexican citizen looking for work can pay a fee to a coyote to traverse our border, what is to keep a terrorist that would do us harm from doing the same thing?

Answer. ICE recognizes that criminal organizations operating worldwide are responsible for smuggling and trafficking tens of thousands of illegal aliens and thousands of pounds of illegal narcotics into the United States. These organizations generate millions of dollars in illicit profits that are moved through wire services, laundered through front businesses and transported out of the country. By exploiting vulnerabilities in border integrity, criminal organizations, whether they smuggle humans, illegal narcotics, illegal arms, or other contraband, are an unquestionable threat to the security of the United States.

ICE has developed a full range of investigation and enforcement methodologies to confront the problem at every point—in source and transit countries, on the seas, at the Nation's borders and ports, and in the U.S. interior. In U.S. embassies throughout the world, ICE Attachés work with consular officials and with foreign law enforcement to better coordinate investigations, gather intelligence and follow the money trail to seize millions of dollars in profits from these organizations. ICE

is also integrating intelligence and enforcement efforts and is mobilizing other governments and international organizations in the fight against human smuggling and trafficking.

ICE has played a significant role in the newly established Human Smuggling and Trafficking Center (HSTC). The HSTC is a joint initiative between the Department of Homeland Security, the Department of State, the Department of Justice, and members of the national Intelligence Community. The HSTC serves as an intelligence fusion center and information clearing-house, with the goal of converting intelligence into effective action.

TEMPORARY WORKER PROGRAM AND BACKLOG ELIMINATION PROGRAM

Question. I remain very concerned with the so called Temporary Worker Program that the President has proposed. Last January, we heard about this program and despite the claims to the contrary it seemed a lot like amnesty. The only difference I can see is that the illegals must have jobs in the United States. Beyond that, these people will be given permission to work and stay even if only temporarily, in the United States despite the fact that they are under the law, criminals. I told you last year that I do not believe in rewarding bad behavior and I still feel the same way today. Under this plan, over 8 million people would have an instant status adjustment. I find this particularly troubling considering the severe backlog of people who are following the law and waiting sometimes years to be allowed to come to the United States.

Director, I know you spoke about the efforts to eliminate the backlog in your testimony and I do appreciate the progress made, but there is much more to be done.

What are we going to do to rectify these problems?

Answer. The President has stated a Temporary Worker Program (TWP) must be guided by four basic principles: that America must control its borders; that immigration laws should serve the economic needs of our country; that we must not give unfair rewards to illegal immigrants in the citizenship process or disadvantage those who came here lawfully, or hope to do so; and, that new laws should provide incentives for temporary, foreign workers to return permanently to their home countries. In designing such a program, we must remain mindful of these principles—and, in doing so, address the common and important concerns that you point out.

The President is also committed to achieving our backlog elimination goals by the end of fiscal year 2006, which USCIS is on track to achieve. A well designed and managed and funded Temporary Worker Program would not adversely affect our backlog elimination efforts. To ensure this outcome, the TWP program design must be cognizant of a variety of factors, including current benefit authorities, options for cost recovery via fees, eligibility criteria, employer/government partnership opportunities, and application process requirements.

Question. I understand that the backlog at different service centers varies, in some cases by months if not years, what is the problem and how do we fix it?

Answer. USCIS has recently submitted a report to the Congress on this subject, which speaks to a staffing analysis recently completed that will help guide the distribution of resources to ensure that Service Centers can meet and maintain backlog elimination goals.

Question. I am also painfully aware that my abilities to assist my constituents through casework has been greatly hindered since at least September of 2003 when the Alabama Delegation contacted the Secretary regarding staffing at your Atlanta office. To date, my staff has trouble receiving prompt replies to inquiries made in Atlanta. Often we can do little more than provide them the information they already have available to them through your website. What can we do to ensure that congressional inquiries to your service offices are acted on promptly?

Answer. USCIS places a high priority on effectively serving its customers. Members of Congress and their staff often contact the agency in order to facilitate the resolution of constituent immigration casework. Many times, it is through a congressional inquiry that a case that has gone off track is identified and resolved. Often these inquiries can help us identify trends where changes in operational practices or policies would be appropriate.

Each USCIS District Office and Service Center has staff dedicated to working with congressional staff. USCIS Congressional Relations has established national standards for responding to congressional inquiries. Telephonic inquiries should be acknowledged or resolved by close of business the next business day, written inquiries should be responded to within 30 days and email inquiries should be responded to within 10 days. Atlanta has been meeting these standards. Still, there are extenuating circumstances where the complete resolution may take longer or where there may be information identified in national security background checks that

cannot be disclosed to congressional offices on individual applicants in order to ensure that ongoing investigations or national security are not compromised.

When we identify a customer service or operational problem specific to a particular field office, a multi-programmatic Field Assessment Team is deployed to undertake a comprehensive assessment of operational effectiveness and responsiveness identifying areas needing improvement, action plans, and specific follow up. In the case of the Atlanta District, such a study was conducted and follow up takes place on a monthly basis. In addition, USCIS has conducted a field study to determine workload and workforce allocation. Through this study, many offices were identified as understaffed and new staff is being hired. As a result of this study, the Atlanta District will be hiring new adjudications staff this year. As new staff come on board and backlogs are reduced, the need for congressional inquires should likewise diminish. The Atlanta District has informed us that they are current with all congressional inquires. If there are any outstanding cases within your office we would be happy to work with your staff on resolving those cases.

IMPORTED SHRIMP INDUSTRY

Question. I know actions are being taken against the imported shrimp industry in response to a dumping determination by the ITC and Dept. of Commerce. Can you tell me what efforts ICE and CBP are being taken in regards to the dumping of shrimp?

Answer. Although the Department of Commerce (DOC) and U.S. International Trade Commission (ITC) share the joint responsibility for antidumping and/or countervailing duty (AD/CVD) orders, the responsibility for the administration and enforcement of these orders belongs to Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE).

In July 2004, CBP amended its continuous bond guidelines specifically for agriculture/aquaculture AD/CVD merchandise as a response to the high-risk nature of these imports. A significant number of shipments were found to have circumvented the AD/CVD cases through incorrect country declarations, undervaluation, and insufficient surety bond coverage, thereby preventing CBP to collect the appropriate duties and make the proper distributions.

The first new case affected by these amended guidelines is shrimp from China, Vietnam, Thailand, India, Ecuador and Brazil. CBP has performed a risk-based analysis on the continuous bonds used by importers of this product to identify circumvention schemes and sham companies. To date this effort has been successful, with CBP revoking over 100 continuous bonds for failing to respond to requests for information. CBP has also worked closely with many importers who are willing to comply with the new bond guidelines to appropriately set new bond amounts to cover the potential financial risk associated with the AD/CVD entries. In addition, CBP is also monitoring imports associated with this case on a monthly basis to identify new importers, misuse of more favorable AD/CVD rates, misdescription of goods, all to avoid paying proper AD/CVD duties.

CBP is also deploying field officers located at Southeast Asian attaché offices to determine if the production capabilities exist for this commodity. When problems are discovered, CBP will make the appropriate referral to ICE for further investigation and action.

BORDER PATROL VEHICLES

Question. As you know, the fiscal year 2005 Homeland Security Appropriations conference report calls for a comprehensive border patrol vehicle fleet management plan by February 8, 2005. Can you please inform the Committee of the status of this report, and specifically the findings with respect to extreme terrain border regions?

Answer. CBP has developed a draft comprehensive plan that was delivered to the Committee on June 28, 2005. Field implementation of the extreme terrain program has begun. The Program consists of four steps: (1) terrain mapping; (2) the evaluation and development of an off-road vehicle fleet; driver training; and sector management orientation. The first step, terrain mapping, involves retrofitting severe and enhanced mobility vehicles with specialized equipment to measure and pinpoint terrain severity using a global positioning system. Agents who have received advanced off-road training operate the vehicles in performing their regular duties, and CBP thus obtains accurate information about terrain severity that will be used to develop the optimal off-road fleet. A total of 10 Border Patrol Sectors were selected for the terrain mapping step in this Program. Mapping started in San Diego Sector in June 2004, and has been expanded to include the El Centro, Yuma, and Tucson

Sectors. The following additional Sectors are scheduled to begin mapping this fiscal year: Marfa, El Paso, El Rio, Laredo, McAllen, and Blaine.

QUESTIONS SUBMITTED BY SENATOR ROBERT C. BYRD

VISA WAIVER PROGRAM: FURTHER EXTENSION

Question. The Enhanced Border Security and Visa Entry Reform Act of 2002, which President Bush signed into law on May 14, 2002, established October 26, 2004, as the deadline by which the 27 existing "visa waiver" countries must have machine readable passports in order for their citizens to enter the United States without a visa. The Congress passed legislation last year pushing back that deadline until October 26, 2005.

Does the Department believe that additional time is required for these visa waiver countries to come into compliance with the machine readable passport requirements? If so, has authorizing legislation to achieve this goal been introduced?

Answer. The Enhanced Border Security and Visa Entry Reform Act provisions are related to machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with applicable biometric and document identifying standards established by the International Civil Aviation Organization. Last year the Administration requested a 2-year extension of the deadline requiring Visa Waiver Program (VWP) nationals to present biometric passports. Congress provided a 12 month extension to give countries designated to participate in the VWP additional time to implement the required passport changes. Given that, DHS and DOS have continued to work closely with VWP participants to review the progress that has been made toward compliance with the new requirement and deadline. We will be able to report on this progress to Congress shortly, though there are still concerns with the current deadline. I look forward to working with you to determine the best solution to both enhance the security of the VWP and enable facilitation of legitimate travel.

Question. Former Secretary Ridge stated in one of his departing interviews that the United States most likely should impose the same requirements regarding biometric identities on U.S. passports. Has the machine readable requirement imposed on foreign visas resulted in negative treatment of U.S. travelers abroad?

Answer. The Visa Waiver Permanent Program (Public Law 106–396) imposed a requirement that VWP travelers have machine-readable passports (with the biographic, not biometric, data being available in a standard manner) for VWP entry on or after October 1, 2007, and that participating VWP countries certify that they are issuing machine-readable documents no later than October 1, 2003. Public Law 107–56, the USA PATRIOT Act of 2001 advanced the deadline for use of machine-readable travel documents by VWP applicants from October 1, 2007, to October 1, 2003, but provided for the Secretary of State to waive the requirement until October 2007. In September 2003, the Secretary extended the deadline for individuals to present machine-readable documents to October 26, 2004. The requirement for nationals of VWP countries to present machine-readable passports to enter the United States under the VWP after October 26, 2004, has not resulted in any reported negative treatment of U.S. travelers abroad.

Additionally, U.S. visas now contain biometrics (i.e. two fingerprints and a digital photograph). European Union nations are discussing options for implementing biometric visa programs as well.

IMPACT OF BUSH AMNESTY ON BACKLOG REDUCTION/WORKLOAD

Question. Your agency's budget request states that, if Congress provides the minimal discretionary funding you are requesting, you are on track to meet the goal of reducing to 6 months the processing backlog for immigration documents.

The President continues to advocate for an amnesty for illegal aliens already resident in this country under the guise of an immigration reform proposal. I am concerned about the impact on your meeting these backlog reduction targets of any immigration proposal. We discussed this issue at last year's hearing, and you responded that any impacts on your agency's goals and operations would depend in large part on what Congress did in response to the President's immigration "reform" proposal. He raised the immigration issue again in his State of the Union address. However, we in the Congress continue to await his "proposal". When will Congress get the President's immigration reform proposal and what impact would his immigration "proposal" have on your backlog reduction proposal?

Answer. The President has outlined his vision for a Temporary Worker Program (TWP) and said that it must be guided by four basic principles: that America must

control its borders; that immigration laws should serve the economic needs of our country; that we must not give unfair rewards to illegal immigrants in the citizenship process or disadvantage those who came here lawfully, or hope to do so; and, that new laws should provide incentives for temporary, foreign workers to return permanently to their home countries. The key to processing temporary worker petitions quickly and efficiently is simplicity in the design. A well designed and managed Temporary Worker Program would not adversely affect our backlog elimination efforts. To ensure this outcome, the TWP program design must be cognizant of a variety of factors, including current benefit authorities, options for cost recovery via fees, eligibility criteria, employer/government partnership opportunities, and application process requirements.

Question. Rep. Sensenbrenner has promised to attach his immigration bill (H.R. 418) to the Emergency Iraqi War Supplemental. This bill includes many of the provisions in the original House draft of the Intelligence Reform Act.

Unlike some rhetorical Bush Administration amnesty, the specifics of this legislation are known. If the provisions of this bill are included in the Supplemental or some other piece of legislation, what impact would it have on your agency's abilities to meet your backlog reduction goals?

Answer. This bill would not impact USCIS' ability to meet backlog elimination goals.

CIS LOCAL OMBUDSMAN

Question. Section 452 of the Homeland Security Act called for the establishment of at least one CIS ombudsman's office in each state. Has CIS complied with the Act? If not, when does the Department plan to do so?

Answer. HSA § 452 establishes the Office of the Citizenship and Immigration Services Ombudsman (CISO), an entity independent of USCIS and reporting directly to the DHS Deputy Secretary. HSA § 452(e)(1)(A) states that the Ombudsman shall have the responsibility and authority "to appoint local ombudsmen and make available at least one (1) such ombudsman for each State."

For fiscal year 2005 the CISO is authorized a total of 24 full-time employees (FTE), and the majority of these employees are planned to be onboard during the third quarter of the fiscal year. For fiscal year 2004 the CISO was authorized a total of eight (8) FTE. The fiscal year 2006 Budget maintains the CISO at the 24 FTE level.

The CISO has established a "Local Ombudsman Pilot Program" which is partially staffed at present but planned to be fully staffed by April 30, 2005. The pilot program is to design and develop a workable local ombudsman office which will have specific operational responsibilities over a defined geographic area. The pilot program will establish personnel certification and training requirements, determine liaison responsibilities and limitations, finalize facilities requirements and provide a controlled model for future local ombudsman office placements. The pilot program will commence upon the arrival to CISO of the new hire personnel to complete the staffing of the pilot local ombudsman office ("Beta Office"). The pilot program is estimated to last for a minimum of 9 months, however that time may expand or contract depending on the results attained. The following is a list of tasks to be accomplished during the pilot program:

—Develop personnel job descriptions based on actual job requirements.

—Conduct a task and skill analysis for each job position to determine the required skills and knowledge for incumbents, as well as to determine individual training requirements for incumbents.

—Design and develop a local ombudsman training and certification program.

—Determine the requisite support equipment necessary for local ombudsman operations.

—Determine the most efficient data transfer arrangement between the Beta Office and the Ombudsman Information Management System (OIMS) to allow for: (1) inquiries and USCIS actions to be received by the Beta Office from OIMS; (2) Beta Office inputs to OIMS; (3) and statistical data and analyses provided in both directions.

—Develop and establish inter-office and intra-office liaison methodologies and procedures, with particular emphasis on: (1) Beta Office to Analysis Branch; (2) Beta Office to Executive Officer staff; (3) Beta Office to OIMS staff; (4) Beta Office to USCIS office(s) in geographic area of responsibility; and (5) Beta Office to individuals/employers as appropriate.

—Develop reporting vehicles for Beta Office operations and productivity.

—Baseline Beta Office operations, duties and tasks under appropriate quality assurance standards.

—Develop and produce procedural manuals to baseline Beta Office operations, duties and tasks.
—Other tasks to be identified throughout the pilot program duration.

NATIONAL BORDER SECURITY ASSESSMENT

Question. The Heritage Foundation issued a December 13, 2004 report entitled "DHS 2.0: Rethinking the Department of Homeland Security," which made a number of recommendations. One of them recommended that the Department of Homeland Security "conduct a national assessment of the resources required for effective border security."

Given the comments by Deputy Secretary Loy and other about the threat facing our borders from a variety of groups, including Al Qaeda, is the Department actively conducting such an assessment and, if not, why not?

Answer. Under the goal of Prevention within the United States Department of Homeland Security Strategic Plan, one of the primary objectives is to: "Secure our borders against terrorists, means of terrorism, illegal drugs and other illegal activity. We interdict terrorist activities by targeting unlawful migration of people, cargo, drugs and other contraband, while facilitating legitimate migration and commerce. The Department will enforce border security in an integrated fashion at ports of entry, on the borders, on the seas and before potential threats can reach our borders. Through the continued deployment of the appropriate balance of personnel, equipment and technology we will create "smart borders." Not only will we create more secure United States borders, but in conjunction with international partners, we will extend our zones of security beyond our physical borders identifying, prioritizing and interdicting threats to our Nation before they arrive. We will develop and provide resources for a cohesive, unified enforcement capability that makes our border security effective, smarter and stronger."

DHS operating elements all share in this requirement and are conducting assessments within their area(s) of responsibility. For example, the Border Patrol has developed America's Shield Initiative, which will methodically assess the highest risk illegal border crossing corridors and, taking into account the topography and other natural barriers, allocate an efficient suite of aerial or ground sensors, personnel and equipment, to best secure the areas between the ports of entry. At the ports of entry, CBP is using and developing enhanced targeting systems and personnel to inspect the highest risk cargo, people and conveyances. In addition, radiation portal monitors are being deployed at our ports to screen cargo for potential weapons of mass effect. One of the tools enforcement officers at the border also employ is the United States—Visitor and Immigrant Status Indicator Technology (US-VISIT) program which incorporates biometrics (finger scans) into entry documentation to ensure we are only letting in those visitors with valid visas who have been cleared against terrorist watchlists and data bases holding fingerprints for criminals. Our national drug control strategy and related annual drug budget also contains information on the trans-national drug threat and resources devoted to combating this problem which complements our border security initiatives. These are a few examples of the family of plans, periodic reviews, acquisitions and programs that collectively contain the assessments and resource requirements for national border security. Annually, those requirements work their way through the budget process producing allocations to address the highest priority security concerns.

IMMIGRATION ENFORCEMENT

Question. Last year, Congress provided $5 million for a worksite enforcement program. For fiscal year 2006, you are requesting $18 million for the same purpose. How have you used the fiscal year 2005 funds? Please describe how the requested fiscal year 2006 funds will contribute to immigration enforcement.

Answer. ICE will increase its presence at worksites, concentrating on employers in specific industries and geographical areas who intentionally violate the law or who have historically hired large numbers of unauthorized workers. ICE will also coordinate with Citizenship and Immigration Services to improve and expand verification services (Basic Pilot Program) to employers nationwide pursuant to the Basic Pilot Program Extension and Expansion Act of 2003.

DETENTION BEDSPACE

Question. For the current fiscal year, Congress provided funding to fill 20,660 detention beds—yet the total beds that you are filling each week thus far is averaging 2,000 below the funded total. Why are these beds not being filled? What types or categories of aliens are not being held?

Answer. ICE Detention and Removal Operations (DRO) is detaining within its budget.

National security cases and criminal aliens are ICE's priority in immigration enforcement. Daily, ICE is at 100 percent capacity of its available allocated funding for detention bed space, the majority of those detained being criminal aliens. This aggressive enforcement posture is reflected in last year's record 160,284 alien removals, including record 84,400 criminal aliens removed from the United States. ICE conducts case-by-case determinations on who will be processed for removal and who will be detained or released. ICE must also carefully consider the conditions of release and factor in community safety especially with regards to criminal aliens. ICE will continue to aggressively enforce immigration laws against criminal aliens and other aliens who pose security threats to the country and expects to continue to achieve increased removals.

Question. Please provide the cost assumptions ICE would use regarding hiring the first year (fiscal year 2006) authorized level in the Intelligence Reform Act (800) for ICE investigators as well as the fiscal year 2007 annualization of those positions. Also, please provide the same information for the costs associated with meeting the first year authorized levels for detention bedspace (8,000).

Answer. The fiscal year 2006 Budget includes substantial increases for increased detention and removal activities. The fiscal year 2006 Budget includes $90 million for detention beds and additional detention and removal officers. This increase will fund 1,920 beds. In addition, the Budget provides $1.5 billion for detention and removal activities, $236 million (19 percent increase) over the 2005 enacted level. In addition, it also includes $39 million for the detention and repatriation costs of the Arizona Border Control Initiative. In addition, 140 new Special Agents will also be hired.

INVESTIGATIONS OF ARMS EXPORT CONTROL ACT VIOLATIONS

Question. The Department of Justice published revised regulations in the November 15, 2004 Federal Register that suggested that DOJ—not ICE—will have the lead role in investigations regarding illegal arms exports. I understand that in late December, you issued a message which stated, in part, "In recent weeks some media reports have suggested that ICE may be ceding some of its authority to investigate violations of the Arms Export Control Act, and other export laws. I am writing today to inform you that nothing could be further from the truth."

This seems to be another troubling example of this new Department's willingness to cede authority to other Departments for some of the traditional roles played by its component parts over the years. The Secret Service had to assert its authority as the primary protector of the currency a few years ago and the Department lost some of its lead role in terrorist financing when former Secretary Ridge signed a Memorandum of Understanding with the former Attorney General. Even the Department's central role in coordinating terrorist threat information was lost—via Executive Order—almost before the ink was dry on the President's signature of the bill creating the Department.

Please explain for the subcommittee the specific roles played by DHS—and ICE in particular—and DOJ in arms export investigations.

Answer. For over 25 years, U.S. Immigration and Customs Enforcement (ICE), has effectively investigated violations of U.S. export control laws. The export control laws enforced by ICE include the AECA, the EAR (concurrent jurisdiction with the Department of Commerce), the International Emergency Economic Powers Act and the Trading with the Enemy Act. ICE uses its border search authority, certified undercover operations and U.S. money laundering statutes as additional tools to prosecute export violators and to assist in the identification and seizure of criminal proceeds of specified unlawful activities. As a result, ICE has successfully investigated hundreds of significant export violations.

ICE will continue to vigorously pursue criminal violations of the export laws and will work jointly with the FBI in export investigations that have a nexus to FCI.

IMPACT OF THE ICE BUDGET SHORTFALL

Question. In the fall of 2003, Congress began calling for the Department to respond to the fact that ICE had insufficient resources to perform its numerous immigration and other investigative duties. In both the fiscal year 2004 and 2005 Appropriations Acts, Congress stepped up to the plate and provided Immigration and Customs Enforcement with more funds than requested by the President to deal with the shortfall.

Yet even with the full acknowledgement that ICE does not have sufficient funding, and that the shortfall has hampered its mission and damaged the morale of its

agents, the President has refused to request supplemental funding to make ICE "whole" and to put it on a sound financial footing.

Immigration and Customs Enforcement should be able to move forward, secure in the knowledge that it has the funds necessary to robustly investigate arms smugglers, terrorists, money launderers, child predators, as well as enforce existing immigration laws.

However, ICE has been forced to take dramatic steps—including freezing hiring, stopping training, and limiting travel—for more than a year in order to live within its constrained budget. The hiring freeze and other spending restraints remain in place nearly 6 months into the new fiscal year. And now we are being warned that ICE faces a funding gap of nearly $300 million this year.

Mr. Secretary, will you end fiscal year 2005 with fewer investigators than you started with at the beginning of Fiscal year 2004? How has that reduction impacted your mission?

Answer. The pending reprogramming will give ICE the ability to end fiscal year 2005 with at least the same, if not higher, level than fiscal year 2004. While ICE has been working through significant challenges during the past 2 years, at the same time, ICE has been achieving unparalleled success in its mission areas. During fiscal year 2005, ICE will continue to work through its challenges and accomplish its critical mission.

Question. Did you seek a supplemental to address the shortfall?

Answer. The proposed reprogramming submitted on March 12, 2005, is sufficient to address the financial requirements of ICE.

CONTAINER SECURITY INITIATIVE: EXPANSION AND REGULARIZATION

Question. I have long been a supporter of the Container Security Initiative, or CSI. This program stations CBP personnel at participating foreign seaports to target and inspect ocean-going shipping containers prior to their being loaded on U.S.-bound vessels. While it was initially skeptical of the program, and reluctant to support the funds the Congress provided to begin its implementation, I am pleased that this Administration has embraced the CSI.

The Administration seeks a modest increase of only $5.4 million for the CSI for a total fiscal year 2006 request of almost $139 million.

During visits to some of these ports, my staff has been impressed with the generally cooperative relationships that have been formed between the CBP personnel and their host country counterparts. As they work together and develop increasing levels of trust, the mutually beneficial aspects of the CSI program to both our country and theirs become apparent. However, the one constant refrain we heard from both CBP and host-country officials was the fact that our people are generally sent over on a temporary basis. They are concerned that once the relationships have matured during the months that the CBP personnel are at a port, they are rotated out and the "trust-building" process must begin again.

Could the effectiveness of the CSI be improved by resolving this temporary duty situation? What are you and the Department doing to ensure that CBP personnel based overseas for CSI implementation are able to stay at a port for a healthy period of time? Are there problems with our State Department representatives that need to be addressed? If so, has this been discussed by Secretary Chertoff with Secretary Rice?

Answer. CBP is transitioning CSI temporary personnel to permanent status. This process requires DHS to coordinate with Department of State (DOS) as required by National Security Decision Directive 38 (NSDD–38). DOS negotiates the placement of permanent personnel at foreign duty posts and also negotiates the appropriate level of Privileges and Immunities (P&I) that will be granted by the host government on behalf of all United States Government agencies.

CBP is currently working with DOS to secure the placement of CSI personnel into a permanent status with the appropriate level of P&I. The DOS has placed a high level of priority on assisting CBP with this initiative.

Question. Without naming any ports or countries, my staff has also heard that some participating ports are often very reluctant to cooperate with our requests for more robust inspection and screening of containers. If this is indeed the case, has consideration been given to lodging formal complaints with the host government—or even to suspending a specific port's participation in CSI?

Answer. There are currently 35 operational CSI ports. The standard operating procedures for these CSI ports are in part governed by a jointly signed Declaration of Principles, in which the host government agrees to pre-screen containers that pose a risk for terrorism.

It is also understood that due to host government sovereignty, the final decision on container examinations is at the discretion of the host government. However, CBP has authority to issue no load order for those who refused inspection.

The CSI program has made significant progress in reaching agreement with host government agencies on what constitutes a high-risk container warranting an examination.

Challenges still exist at one CSI location with regard to common and agreed upon definition/designation of high-risk containers warranting examination(s).

CBP is confident that with the high percentage of CSI locations operating very effectively that continued progress will be made in this one location. CBP has, and continues to consult with State Department (including the U.S. Embassy in this location) to enhance the CSI operation.

CBP has contemplated the alternatives and is receiving full support from all Departments and Agencies in making CSI efficient and effective.

IMPACT OF LATE DUTY COLLECTION ON CRAWFISH INDUSTRY

Question. As mentioned previously, in the past, U.S. industries like the U.S. crawfish industry have discovered only very late in the year that millions of dollars of antidumping duties for some reason have not been collected in their cases against Chinese imports as required by law. And, because CBP's failure to collect these duties has been discovered late in the year, the non-collection problem in these cases could not be addressed in time to enable the industries to obtain their yearly distribution of funds under the Byrd Amendment. As a consequence, the U.S. crawfish industry, for example, last year failed to receive at least $54.4 million it otherwise would have received in duties paid the United States Government by Chinese importers.

It is my understanding that CBP's Office of Information Technology (OIT) is fully capable of running an already existing program much earlier in each calendar year, (meaning by the end of March at the latest), which would enable both CBP and U.S. industries to learn, much earlier, if millions of dollars in duties are not being collected by CBP from U.S. importers of foreign, dumped products.

Why can't CBP's Office of information Technology determine by the end of this month if there are cases in which CBP is not collecting duties owed the United States Government and make that information publicly available as early as possible?

Answer. CBP has responded to the revenue risk posed by the inability to collect certain AD/CVD duties through several means, one of which is the monitoring the AD/CVD bills and collections on a more regular basis. For the distribution of these funds to take place timely, it is necessary not only to monitor the timely collection of AD/CVD duties but also to ensure our revenue collection system is protected from possible circumvention and corporate solvency schemes designed to enter AD/CVD goods into the U.S. market with the intention of never paying the proper duties at time of liquidation.

On a monthly basis, CBP is performing a risk-based review of outstanding bills for AD/CVD duties. The information has proven effective in identifying high-risk companies for AD/CVD evasion as well as improve the timeliness of our reviews. CBP is also focused on the long-term issue of the company's financial solvency and their ability to pay outstanding AD/CVD bills. The continuous bond guidelines for imports of certain agriculture/aquaculture imports were amended in July 2004, to address just such an issue. Working with the Department of Commerce, we are addressing the AD/CVD issues that pose the greatest risk.

OVERTIME PAY WHILE RECEIVING TRAINING

Question. I understand that since January 2, 2002, your bureau has not compensated CBP officers who train 6 days a week at the Federal Law Enforcement Training Center. In essence, this means that hundreds of newly trained CBP officers have had to work 6 days a week for up to 12 weeks without any compensation for overtime.

I support your "One face at the Border" initiative and acknowledge that the merging of certain legacy personnel into a new agency requires intensive training. But I think you would concur that this should not come at the expense of basic compensation for these professionals.

How do you plan to correct the current overtime pay problem for these CBP officers who were trained between January 2002 and October 2004?

Answer. CBP is also concerned about equitable compensation for the employees who were engaged in training at the Federal Law Enforcement Training Center (FLETC) on a 6-day schedule. As you are aware, the Federal Law Enforcement

Training Center (FLETC) determined that the 6-day schedule was a necessity post-September 11 in order to accommodate the robust training needs of law enforcement personnel.

The Government Employee Training Act prohibits the Federal agencies from compensating employees with overtime while its employees are engaged in training by, in or through government or non-government facilities (5 USC, 41). There are only a very few exceptions to this broad legislative prohibition, and the CBP has used these, where possible, to legally pay our employees so situated.

Chief amongst these exceptions is a different set of regulations that applies to employees covered by the Fair Labor Standards Act (FLSA). Legacy INS inspectors, prior to conversion to the CBP Officer position and COPRA compensation, were covered by FLSA. We were therefore able to retroactively compensate them for the overtime worked on the 6 day during the FLETC training; these retroactive payments were made in December 2004. Because the agency determined that legacy Customs Inspectors were covered by COPRA and therefore exempt from FLSA, payment for the 6 day was not appropriate. The different outcomes regarding payment of overtime resulted from the fact that these groups of employees were covered by different laws at the time that the training occurred.

The National Treasury Employees Union (NTEU) challenged the agency through arbitration concerning this issue, and the agency's legal interpretation was sustained by the arbitrator. This is a complex matter, and there is litigation still pending. It is also important to note that effective October 1, 2004, FLETC returned to a 5-day training week

CONTAINER SECURITY

Question. In December 2004, the Department unveiled a draft cargo security strategy. This strategy stated that the Department proposes to adopt a "zero-tolerance policy" regarding the arrival of weapons of mass effect at our Nation's borders. I concur that preventing these weapons from entering the United States should be a priority. I always assumed that it was.

The conference report accompanying the fiscal year 2005 Homeland Security Appropriations Act notes that over $200 million has been spent over the past 3 years on various projects designed to secure cargo containers entering this country. It also calls on the Under Secretary for Border and Transportation Security to—among other things—report to the Congress no later than February 8, 2005 on which DHS entity will have primary responsibility for cargo container security and the setting of shipping industry standards. To date we have not received this report. I assume your agency was closely involved in the drafting of this report.

How closely were you involved in the drafting of the report and can you give us a sense of what it might recommend?

Answer. In support of the Department's cargo security strategy proposal to adopt a "zero-tolerance policy" regarding the arrival of weapons of mass effect at our Nation's borders, CBP has deployed various types of radiation detection technology nationwide with the ultimate goal of screening 100 percent of containerized cargo for radiation.

CBP has provided significant input to the draft report on Cargo Container Security, including information regarding the current status of major CBP initiatives addressing cargo security. In providing summary reporting, CBP outlined the desired end state; namely, securing and improving operations at existing ports; expanding operations to new critical international seaports and encouraging global efforts to enhance supply chain security.

Question. Do you know when the Congress will receive the report which is now nearly 1 month overdue?

Answer. The final report was submitted to the Committee on June 8, 2005.

AMERICA'S SHIELD INITIATIVE

Question. This Department seems obsessed with selling old wine in new bottles. The visa tracking program known for years as "Entry-Exit" became "US-VISIT". The Office for Domestic Preparedness became the Office for State and Local Government Coordination and Preparedness. Now the Border Patrol's Integrated Surveillance Information System, or ISIS, has been "re-branded" as "America's Shield Initiative"—or ASI. Regardless of the new names for these old programs, the fact remains that our borders need to be protected.

America's Shield Initiative is supposed to implement the Border Patrol National Strategy to strengthen U.S. borders to prevent the entry into the United States of terrorists and terrorist weapons, smugglers and illegal aliens, narcotics and other contraband.

Our borders are under attack. The President's own experts know and are extremely concerned about the threat terrorists pose to our borders. In written testimony before the Senate Intelligence Committee on February 16, Deputy Secretary Loy cited recently received information as the reason for his concern about the threat facing the Mexican border. He called it a "very serious situation."

Given this threat, why does the request include only $20 million for improved technology on our borders, when CBP staff have estimated the full cost to be $250–300 million?

Answer. The total funding for the ASI program in fiscal year 2006 is $51 million, including $19.8 million for new investments. The fiscal year 2006 request for ASI when coupled with investments for additional Border Patrol Agents, helicopter replacements, enhancements to Border Patrol facilitates and tactical infrastructure will provide CBP with a complement of resources that will increase operational control of our Nation's borders.

IDENT/IAFIS UPDATE

Question. The integration of the fingerprint databases created, maintained, and used by the Department of Homeland Security and the FBI—among other Federal agencies—continues to be a priority concern for the Congress and the members of this Subcommittee. It is critical that we know whether visitors to this country pose a risk to our citizens. As you know, the 9/11 hijackers came into the country on student and tourist visas.

Your Border Patrol agents daily compare the fingerprints of illegal aliens apprehended at our borders against these databases. And it is your inspectors who—at a growing number of ports of entry—compare the fingerprints of visa holders and others wishing to enter this country against these same databases via the US-VISIT system.

That is why I was concerned about the latest Department of Justice Inspector General report on this subject. It stated that of the 118,000 visitors daily entering this country who are subject to US-VISIT, an average of about 22,350 individuals are referred for secondary inspection. According to DHS, by the end of this fiscal year, it expects to directly check only about 800 individuals each day against the full FBI fingerprint database known as the IAFIS Criminal Master File. This is less than 1 percent of the 118,000 daily visitors.

Why are we checking less than 1 percent of visitors to this country against the FBI fingerprint data base?

Answer. This response contains information considered Law Enforcement Sensitive and has been provided to the Committee under separate cover.

Question. According to the Justice Inspector General report, the Justice Department will be increasing the FBI's capacity to handle fingerprint checks from 8,000 per day to 20,000 per day by October of this year. Will you be changing your policies so that CBP is fully utilizing that capacity to check the criminal backgrounds of visitors coming into this country?

Answer. DHS and Department of State have found that IDENT achieves their counterterrorism, major law enforcement, and border management objectives in timeframes that meet operational needs for processing at ports of entry. Every day, DHS and DOS run checks on approximately 115,000–120,000 individuals using IDENT. These checks are returned, on average, within 10 seconds at ports of entry for US-VISIT and within 15 minutes for Department of State. Even if IAFIS increases its capacity to 20,000 fingerprint checks per day, it still cannot come close to the number of transactions currently generated by the US-VISIT program. Additionally, IAFIS returns results, on average, at best within 10 minutes, most (such as those transmitted by State) within several hours. Currently, IAFIS does not have the capacity to meet our operational needs for inspecting visitors. However, we are continuing to work with the Department of Justice on finding ways to better integrate IAFIS with our existing systems, such as the successful integration at our Border Patrol stations.

COLLECTION OF DUTIES

Question. Again, two of the problems that CBP has exhibited with respect to its administration of the Byrd Amendment are (1) Customs' failure to collect duties rightfully owed; and (2) its failure to pay duties already collected in a timely fashion to eligible U.S. companies and their workers.

With respect to the second problem, Customs sometimes holds, in what are called "clearing accounts," duties that are collected over many years—but for which the agency is awaiting final "liquidation instructions" from the Commerce Department

prior to distribution. Often, the Commerce Department claims that such instructions have been sent, but CBP does not know they have been sent or never receives them.

It has been proposed that one solution to this problem would be for CBP to publish the amount of funds held in CBP's clearing accounts, by administrative review period, so that CBP and Commerce can work together to determine which funds should have been liquidated and be available for distribution to eligible U.S. producers. CBP, in certain circumstances, has provided such information to Members of Congress upon request, but has refused to provide such information generally.

Will you commit to identifying (i.e., publishing) the amount of funds held in clearing accounts by administrative review period?

Answer. The CBP program is designed to generate a bill and collect the appropriate duties following the liquidation of each entry summary. However, importers are provided the opportunity to appeal these decisions, which may involve working with the Departments of Commerce and Justice to ultimately collect these AD/CVD duties. During this time, estimated duties collected on the entry summary are held pending the final liquidation and collection of these duties before they may be disbursed in accordance with the Continued Dumping Subsidy Offset Act.

To ensure transactions are not inadvertently held and made available for disbursement, CBP initiated a plan to review and liquidate entries that may have been inadvertently held in clearing accounts. CBP provided extensive data to Commerce regarding entries by administrative review period that remain unliquidated. Feedback from Commerce on this analysis allowed CBP field offices to finalize 11,000 old AD/CVD entries whose liquidation makes $12 million eligible for disbursement.

This process also shed light on the cause of the backlog. Over two-thirds of old unliquidated entries (10 years old or more) resulted from a weakness in communicating liquidation instructions from Commerce to CBP. In most instances, CBP is holding old AD/CVD entries with import scenarios not covered by any published Commerce instructions. This is particularly true where instructions are contingent on a complex mix of importer, exporter and/or producer. In fiscal year 2005, CBP is concentrating on the liquidation of all remaining AD/CVD entries entered prior to 1995 that remain suspended.

We are committed to working closely with Commerce to ensure that CBP promptly receives and acts upon all liquidation instructions issued. This will enable CBP to act as promptly as possible to initiate liquidation of the affected entries. This could potentially include a case-by-case comparison of orders.

Question. Will you commit similarly to identifying the reasons for the lack of liquidation in cases where liquidation has not occurred for more than 4 years, and provide specific information with respect to those cases showing the amounts that remain unliquidated accompanied by an explanation of CBP's understanding of why the amounts have not been liquidated?

Answer. The antidumping and/or countervailing duty (AD/CVD) modules within the Automated Commercial System (ACS) do not provide information by administrative review periods; therefore, CBP cannot track entries this way. Although one module exists to track liquidation instructions by review period—the Department of Commerce (DOC), who has sole responsibility for the AD/CVD modules, has not consistently provided this information.

A liquidation clean-up project was initiated by CBP in response to the Office of Inspector General (OIG) audit on CBP's implementation and management of the Continued Dumping Subsidy Offset Act (CDSOA). The OIG report expressed concern over CBP's unliquidated inventory of 1 million entries and states "clearing up the liquidation backlog should be a priority given the substantial dollars involved." At present, CBP is holding an "official" inventory of 2.2 million suspended AD/CVD entries covering 593 cases. According to the AD/CVD duty module within ACS only 327 of those cases are current, the rest are either revoked (once open, but subsequently closed), terminated (investigated, but never issued), or in some stage of investigation (prior to a decision on issuance). CBP believes that many of these entries can be closed out.

CBP provided extensive data to DOC regarding entries that remain unliquidated despite the fact that their associated AD/CVD cases were either terminated revoked or did not have instructions issued for a specific review period. Feedback from DOC on this analysis allowed CBP field offices to finalize 11,000 old AD/CVD entries whose liquidation makes $12 million eligible for disbursement pursuant to the Continued Dumping Offset Act of 2000.

The liquidation clean-up project also shed light on the cause of the backlog. Over two-thirds of old unliquidated entries (10 years old or more) resulted from a breakdown in the liquidation instructions from DOC to CBP. In most instances, import specialists are holding old AD/CVD entries with import scenarios not covered by any published DOC instructions. This is particularly true where instructions are contin-

gent on a complex mix of importer, exporter and/or producer. In fiscal year 2005, CBP is concentrating on the liquidation of all remaining AD/CVD entries entered prior to 1995 that remain suspended. Another reason that monies remain in the "clearing accounts" and are unavailable for distribution via CDSOA are the number of protests on bills issued by CBP. Payment of a protested bill is deferred until the protest decision is rendered. Currently many protests of AD/CVD liquidations are suspended pending the final decision by the Federal Appeals Court on International Trade.

TRAINING OF CBP INSPECTORS

Question. With the creation of the CBP Officer position along with the "One Face at the Border Initiative", how does the CBP plan to make sure that one front-line employee can essentially perform job functions that were previously done by 3 different inspectors? Does DHS plan to create specialty experts for various legacy Customs and INS disciplines, or will every officer have to know every detail of both Customs and INS laws for both the primary and secondary inspections at the border?

Answer. We are working towards creating an agency-wide law enforcement and national security culture, establishing unified primary inspections at all United States ports of entry and conducting secondary inspections focused primarily on combating terrorism and the traditional missions inherited by Customs and Border Protection. To do this efficiently and effectively, we have built a comprehensive training plan to guide our efforts.

A very stringent 20-day pre-academy and 73-day basic academy training curriculum has been developed for the new CBP Officer. This training gives them the foundation needed to work in the primary setting upon their return to the port, while also giving them a basic understanding of what occurs in the secondary environments. The ultimate goal is to train the new CBP Officer to not only be equally competent in all of the former, individual areas of responsibility, but also to be better able to meet the expanded mission priority of anti-terrorism. Their Academy training is then followed by a rigorous 2-year on the job training program with approximately 40–45 weeks (depending on environment—air, land or sea) of structured training courses. They are given training in stages in order to absorb it and be afforded time on the job to perform the duties and become proficient.

A comprehensive 37 module cross-training program has been built for those officers who previously performed an Agriculture, Customs or Immigration function at the ports. Training is being given to those officers on a "just in time" basis to perform the job they are being asked to do. Instead, CBP has created a curriculum that builds off of each previous module.

CBP does have several courses which are considered to be advanced training and they would include those that involve analytical capabilities and the counter-terrorism response units in our secondary areas. CBP is currently exploring the possibility of having additional areas and courses designated as specialized training classes.

Question. Explain how Customs cargo inspection expertise will not be lost in the transition to the new CBP officer position? Will the new CBP officer be required to thoroughly understand the massive harmonized tariff schedule for goods being imported into the United States as well as being responsible for thousands of pages that comprise the 400 sections of Immigration and Nationality Act, hundreds of pages of INS Title 8 Federal Regulations and the full INS operations inspection manual?

Answer. Currently, CBP's Office of Field Operations is developing, in conjunction with the Office of Training and Development, three separate Cargo cross-training modules for the air, land and sea environments. The primary recipients of this training will be the new CBP Officers and those legacy Immigration Officers new to the cargo environment. The training consists of both classroom instruction on cargo processing, and on-the-job cargo training under the supervision of an experienced CBP Officer. The training consists of reviewing bills of lading, processing all types of entries and conducting cargo examinations. Officers will receive this training on a "just in time" basis as they are assigned to cargo primary.

The expertise on classification using the harmonized schedule still resides with the Import Specialists. CBP Officers are introduced to the harmonized schedule in some of our Customs Secondary training as well as the cargo courses described above. We teach a basic understanding of the tariff, how to locate items, and how to do a basic classification/duty calculation. Final classification and duty calculations are done by the Import Specialist.

It is expected that our training effort for the CBP Officer and CBP Agriculture Specialist will be conducted over the course of many years. CBP policy is that no

officer may perform a function or a part of an assignment without having completed the appropriate training module, systems training and on the job training that are associated with those duties.

Question. The Department's "One Face at the Border Initiative" merged over 18,000 inspectors from the Customs Service, Immigration and Naturalization Service (INS), and the Animal Plant Health Inspection Service (APHIS), into one front line inspector position. As you know, current legacy Customs, legacy INS and the new CBP officers carry weapons and have arrest authority but are NOT considered Federal law enforcement officers. With the demands of the Federal law enforcement officer having evolved over the last decade, do you not believe that including Federal personnel such as Customs and Border Protection Officers, who not only protect our border from illegal drugs and facilitate lawful trade, but must now defend against weapons of mass destruction and terrorism and the risks that come with these added job responsibilities, deserve the recognition and benefits that go with Federal Law Enforcement Officer (LEO) status?

Answer. Customs and Border Protection (CBP) Officers are, in many important respects, law enforcement officers, because they have the responsibility for enforcing laws, making arrests, and performing a critical enforcement and security mission. However, the position does not meet the current statutory definition for coverage under the special retirement provisions, which requires the primary duties to be either investigations of crimes or the apprehension and detention of criminals or individuals suspected of criminal activity.

Question. The final personnel regulations greatly reduce the circumstances where collective bargaining will occur for CBP employees. Can you please tell the committee why the regulations prohibit collective bargaining over basic conditions of work, such as employees' rotation between different shifts or posts of duty, or scheduling of days off, including even post-implementation expedited bargaining? It appears the current procedures for bargaining over basic workplace matters such as scheduling have not hampered the agency's homeland security missions in any way.

Answer. The successful assignment and deployment of the right employees and technology at precisely the right time is critical to the accomplishment of CBP's primary mission of preventing terrorists and implements of terror from entering the United States through and between our ports of entry. As a result, CBP must be able to assign and deploy employees, and to introduce the latest security technologies without delay. To assist in the facilitation of this requirement, the final DHS regulations provide CBP the flexibility to meet operational needs in these areas without subjecting such managerial decision to protracted negotiations and third party review by individuals or organizations who may not have a full understanding of the complexities of CBP's anti-terrorism mission and operational requirements.

However, in order to balance these operational requirements with the interests of employees, the final regulations do provide an important mechanism for CBP to consult with employee representatives regarding the exercise of these flexibilities. Specifically, CBP will continue to inform labor organizations of its policies and procedures in these areas, to meet and discuss their views, concerns and recommendations with regard to the procedures by which these management flexibilities are exercised, and to attempt to reach agreement on such procedures where possible. Furthermore, where CBP institutes significant changes during the life of a collective bargaining agreement affecting the working conditions of employees, the final regulations provide for negotiations with labor organizations in those cases where the change is foreseeable, substantial and significant in terms of impact and duration on the whole or significant portion of the bargaining unit.

This new framework for interacting with its labor organizations will better support and facilitate the accomplishment of CBP's critical national security mission, while providing a viable and streamlined avenue for the expression and consideration of employee interests and concerns.

BORDER PATROL—APPREHENSIONS

Question. On average for the current fiscal year, how many illegal aliens is the Border Patrol apprehending each week? Of those, how many are considered to be criminal aliens or who require mandatory detention bedspace? Of the non-criminal/non-mandatory aliens, what is the average length of their stay in the United States in Border Patrol custody prior to be being removed/expelled?

Answer. The Border Patrol has apprehended 457,900 illegal aliens to date in fiscal year 2005 thru March 11, 2005, approximately 19,908 per week.

Of the total apprehensions to date in fiscal year 2005, 6,171 were determined to be criminal aliens (which equates to about 268 per week). The number of mandatory

detention varies widely. Often the determining factor whether aliens are detained or released on their own recognizance depends on available bed space. The Border Patrol would like to detain all criminal aliens and non-Mexican apprehensions, but currently this is not feasible. The Border Patrol does not detain any aliens beyond 72 hours. Most detainees are turned over to Immigration and Customs Enforcement/ Detention and Removal Office (ICE/DRO) before 72 hours. ICE/DRO has advised us that aliens detained for Expedited Removal are routinely held for 30+ days. Criminal aliens and those required deportation hearings are held from 75–100 days.

BORDER PATROL—STATIONING OF AGENTS

Question. On average, how long does it take to identify, hire, perform a background/suitability check and train a new Border Patrol agent prior to their being posted on the border?

Answer. Advance recruitment for entry-level Border Patrol agents is done on a regular basis in order to have a nationwide standing inventory of eligible candidates who already have passed the written and oral exams, completed pre-appointment requirements (including background investigation, medical screenings, etc.), and are ready for final selection. It generally takes 6 to 8 months following tentative selection for a candidate to be added to the hiring queue for job placement. A candidate's position in the hiring queue is based on the written test score plus any applicable veterans preference points.

When the Office of Border Patrol (OBP) identifies specific positions and locations to be filled, offers are extended to candidates in the hiring queue, their starting dates are established, and their training is scheduled. This process generally takes 2 to 4 weeks. Within a few days of their hire, the trainees are detailed to the Border Patrol Academy in Artesia, New Mexico for 19 weeks of basic training. Upon completion of basic training, the agents are returned to their home duty stations as certified, credentialed and armed agents. Formal post-Academy training continues on the job through the remainder of the first year.

Question. How many Border patrol agents are currently stationed on the Southwest and Northern Borders? How many agents were stationed on each border on September 11, 2001? Prior to 9/11, what was the average placement of BP agents per mile on the Southwest and Northern Borders? What are those numbers today?

Answer. There are currently 10,525 Border patrol agents stationed on the Southern and Northern borders with 9,501 on the Southern border and 1,024 on the Northern border. There were 9,459 Border patrol agents on the border on September 11, 2001, with 9,124 on the Southern border and 335 on the Northern border.

The number of agents on duty per mile varies widely based on risk assessments, traffic patterns, deployed technology in an area and staffing and personnel changes. For example, the evening and night shifts typically have a higher staffing level than the day shift since most illegal intrusion attempts occur during the hours of darkness. As a result of these variables there is no standard average for agents on the border at any given moment.

BORDER PATROL

Question. Please provide the cost assumptions CBP would use regarding hiring the first year (fiscal year 2006) authorized level in the Intelligence Reform Act (2,000) for Border Patrol agents as well as the fiscal year 2007 annualization of those positions.

Answer. The Intelligence Reform Act presents an ambitious and aggressive goal of doubling the size of the Border Patrol Agent cadre over 5 years. For fiscal year 2006, the Act authorizes an increase of almost 20 percent to the number of Agents now on-board. There are practical limitations to the number of Agents that the Border Patrol can efficiently and effectively absorb in a year. These limitations are the result of the existing Border Patrol infrastructure (including training facilities, Border Patrol stations, support personnel, communication systems and vehicle and equipment repair and maintenance facilities) and the numbers of agents that can be brought on annually without undermining the organizational cohesiveness needed for a law enforcement organization like the Border Patrol. Significant investments in the Border Patrol infrastructure are required as a prerequisite to, or at least concomitant with, the increase in the Agent cadre authorized by the Act.

Assuming that the Border Patrol infrastructure receives corresponding budgetary increases, a $697.33 million would be required for fiscal year 2006 and $447.41 million will be required in fiscal year 2007. This includes to costs to effectively hire, train, equip and train each new border patrol agent. In addition, it includes costs for support personnel, infrastructure, relocations, and the IT support necessary to support such an increase.

WAR ON DRUGS—HISTORICAL

Question. During the 1980s, there was a major focus on the "War on Drugs" on the Southwest Border. Additional resources were provided to the Border Patrol and then-Customs Service to engage in this fight. Please provide the total number of Border Patrol agents and Customs Service personnel (per year 1980–1990) as well as the number of those personnel in each agency who were dedicated to the Southwest Border.

Answer. Shown below is a chart reflecting the number of Border Patrol agents and the number of those agents assigned to the southwest border.

BORDER PATROL AGENTS

Fiscal year ending	Nationwide
1980	2,329
1981	2,240
1982	2,227
1983	2,339
1984	2,333
1985	3,023
1986	3,238
1987	3,180
1988	4,074
1989	3,857
1990	3,778

CBP does not have access to personnel data for the 1980–1990 timeframe because the former U.S. Customs Service converted to the United States Department of Agriculture's Personnel System in 1992.

QUESTIONS SUBMITTED BY SENATOR DANIEL K. INOUYE

IMMIGRATION OFFICERS IN LOCAL USCIS OFFICES

Question. Being able to talk to knowledgeable immigration officers in local USCIS offices is an important customer service, especially for elderly or illiterate USCIS customers. Although InfoPass provides a free, easy and convenient alternative to waiting in line, InfoPass has caused confusion for a number of Hawaii customers who were turned away at the local USCIS office because they did not know how to use InfoPass. The InfoPass program assumes that all immigrants are literate, have access to a computer, and are able to type on a computer keyboard. How is USCIS addressing this problem to enable access for elderly or illiterate customers with limited computer access and limited ability to use the Internet?

Answer. USCIS encourages customers who need information about citizenship and immigration benefits and services to begin with our website, or call the toll-free customer service number. That is because many times they can get the information or assistance they need without having to make a trip to one of our offices.

InfoPass is designed to let customers who do need in-person service make an appointment to reduce the time they may otherwise have to wait to be served once they arrive. USCIS prioritizes customers with appointments to try to ensure that they do not have to wait for service.

However, we recognize that not all customers have access to the Internet. We do continue to offer very basic services, such as forms and standard materials, to customers who do not have an appointment. If it is determined that a customer needs a service that we provide by appointment, we will look to see if one is available that day. If not, and the customer indicates they simply do not have the Internet access to be able to make an appointment, we will help them make their appointment for another day.

LIFE ACT

Question. I am aware that the Legal Immigration Family Equity Act (LIFE Act) was enacted into law in 2001 to reduce the separation of immediate family members of U.S. citizens who are waiting abroad for an immigrant visa. The CIS Service Centers were taking approximately 8–12 months to process immediate relative (form I–130) visa petitions. The LIFE Act created a new K nonimmigrant category that allows a spouse or child of a U.S. citizen to enter as a nonimmigrant on a K–3/K–

4 visa to reunite with her family, and then apply for lawful permanent residency while in the United States.

A U.S. citizen can file a K (form I–129F) visa petition for a spouse or child with the National Benefits Center once he files an immediate relative (form I–130) visa petition and receives a notice of receipt from a Service Center. In most cases, the U.S. citizen petitioner files both the I–130 and I–129F, assuming that the I–129F will be processed faster, due to the USCIS' announced policy to implement the LIFE Act. However, petitioners are finding that the National Benefits Center is slow to adjudicate K visa petitions and is taking approximately 7 months. Currently, three of the four Service Centers are processing immediate relative (form I–130) visa petitions faster than the National Benefits Center is taking to process the I–129F visa petitions (California Service Center=60 days; Vermont Service Center=3 months; Texas Service Center=6 months).

The slowness of K–3 processing suggests that the K–3 program is not working as it was intended, which is to expeditiously reunite U.S. citizens with their spouses and minor children. Furthermore, U.S. citizens submitting K visa petitions waste valuable time and money ($165 for each petition) when the program fails to provide them with the service and benefits that were intended by Congress. What steps are being taken to effectively implement the K visa program?

Answer. USCIS recently made a processing decision that caused the situation that we are now facing with Immediate Relative visa petitions and the processing of spousal nonimmigrant visa petitions.

In reviewing our relative visa petition process, USCIS decided that the Service Centers should focus their efforts on relative visa petitions submitted by U.S. Citizens. As a result of these efforts, the Service Centers have done an outstanding job and have decreased processing times for this type of relative visa petitions dramatically.

At the same time, the National Benefits Center (NBC), which processes the K–3 visa petitions, has continued to process K–3 nonimmigrant spousal cases as quickly as resources will allow. The NBC is currently in the process of acquiring more adjudicative staff to focus on this workload. In the short term, NBC will realign existing staff, including utilization of overtime funds, to reduce the pending workload and achieve currency.

Lastly, it has come to the attention of USCIS that if an applicant has both an approved I–130 petition and an approved K–3 petition at the same time, some local State Department Consulate offices make the decision to give the I–130 petition more weight than the K–3 petition. This decision has an impact on the Affidavit of Support and Medical requirements the petitioner must meet before State will issue an immediate relative visa associated with the I–130. USCIS will work with the Department of State to review this situation and identify a remedy to ensure that both types of visa categories are processed effectively.

F2B PREFERENCE VISA PETITION

Question. When a petitioner, who originally filed an F2B preference visa petition, becomes a naturalized U.S. citizen, his petition is automatically given F1 status. For those who file petitions for relatives in the Philippines, they are penalized by becoming citizens because their beneficiaries' waiting period is extended by several years.

Section 6 of the Child Status Protection Act allows a petitioner to opt out of converting to F1 status. The bill was enacted into law several years ago, but those individuals who applied to opt out are still waiting for the Attorney General to implement Section 6. The National Visa Center has informed petitioners that there is no timeframe for when this review will be completed. Can you please comment as to when can we expect this issue to be resolved?

Answer. USCIS is in the process of writing a regulation to codify the Act. We hope it will be published by this summer. In the interim, USCIS has issued a policy memo to provide guidance on adjudicating requests tendered pursuant to Section 6 of the CSPA.

1–800 CUSTOMER SERVICE NUMBERS

Question. I have heard from number of comments by USCIS customers that when they dialed the 1–800 customer service numbers, they received misinformation that led to sometimes fatal errors in their immigration application, because the customer service person is reading a script but is otherwise inexperienced in immigration procedures. Please comment on this customer service problem.

Answer. All contract customer service representatives must take a USCIS approved course, and pass a USCIS approved exam, before they can answer phone calls. The course and exam are designed to ensure that representatives have an un-

derstanding of the terms and language of immigration, and can find the appropriate materials to convey information or offer services to a caller, before they assist customers.

USCIS' commitment to the accuracy and quality of the assistance we offer is reflected in the fact that we require contractors to monitor each representative randomly twice a day to measure their performance against a set of customer service standards. We also have an independent company monitor calls against those standards. USCIS also uses a secret shopper program to test and evaluate performance against a set of future benchmarks for where we want to be in terms of service provision, and each month conduct a random phone survey of callers to get feedback about their experience.

However, as with any verbal interchange we recognize that customers may not recall in its entirety a precise explanation or conversation, may misunderstand an explanation, or that, for all our controls, a representative may not convey the correct or complete answer. We also understand that customers searching for information about citizenship and immigration benefits, which can lead to life changing events, and work to improve our process to ensure that we are giving them all the options and information. One of USCIS' goals is to give each customer more control over the process, and to give them broader direct access to the scripts and other materials which we have available. Thus, we plan to put all of the scripts that we use to answer customer questions on our website so that customers can do their own research, and can print the information to be able to review it rather than just hearing it explained to them. In fiscal year 2005, USCIS plans to release additional standardized fact sheets and brochures, again to give customers direct access and something they can take with them. We plan to make this information available on our website, and in addition will make them available at our local offices, by phone, and through community partners.

QUESTIONS SUBMITTED BY SENATOR PATRICK J. LEAHY

PORTS OF ENTRY IN VERMONT

Question. I understand there are a number of ports of entry in Vermont that will be overhauled in the next 5 years. What is the current schedule for construction at the each of the major ports in Vermont? What, if any, requests has DHS made to GSA for planning or construction projects in Vermont? Of all the border crossings nationwide, what is the typical length of highway before the actual border that is deemed part of the port? How far along the highway do the longest 5 extend into the United States?

Answer. CBP has requested GSA to consider the Ports of Entry at Derby Line (I–91), Richford, and Norton, Vermont for construction in fiscal year 2007. In addition, CBP has requested GSA to begin design in fiscal year 2007 for Richford (Route 139) and Beebe Plain, Vermont with construction to follow in fiscal year 2009.

In regards to the typical distance between the land ports of entry (LPOE) and the international boundary, there are several key factors carefully considered to ensure the safe passage of traffic and the trade while maintaining safety for CBP Officers and the public.

Key factors used to determine the LPOE location relative to the international border are:

—*Line of Sight.*—An adequate line of sight (direction, slope, elevation, and obstacles) must be maintained between operational functions at the LPOE. The distance between the LPOE and the international border should be minimized to ensure that activity in the area is effectively observable.

—*Alignment of Vehicles.*—The alignment of passenger vehicles and commercial trucks preparing to enter through Radiation Portal Monitors (RPM) and License Plate Readers (LPR) on the way to the primary inspection booth is critical. The distance required for safe vehicular alignment leading up to the LPR/RPM is 40 feet for passenger vehicles and 90 feet for commercial trucks.

—*Obstacles.*—There should be no obstacles (buildings, vegetation) located between the LPOE and the international border that would impede the operational effectiveness of the port or degrade safety and security for the CBP Officers and traveling public.

The vast majority of our LPOEs boundaries begin within 100 feet or less of the international border. We do have several locations where the distance is greater as a result of environmental wetlands or other considerations that precluded construction closer to the border. At one location in Minnesota we are planning to be approximately one-half mile from the border but will address security requirements

through the use of video monitoring systems. It is standard CBP policy to maintain a clear line of sight between the operations within the LPOE and the international border to ensure that our officers monitor all traffic entering and departing the United States.

BORDER PATROL CHECKPOINTS

Question. I have received many complaints and concerns from my constituents about the checkpoint that has been established on Interstate 91 in Vermont. One of my constituents, a naturalized citizen who lives in Vermont and works in New Hampshire, has been stopped repeatedly and questioned about his legal status. Other constituents have expressed concern that racial profiling is occurring at the checkpoint. (A) Is there anything you would be willing to do to prevent naturalized citizens from being stopped repeatedly at this checkpoint, such as offering a frequent traveler card? (B) What measures do your officers take to avoid racial profiling?

Answer. Border Patrol traffic checkpoints are operated in accordance with the Constitution of the United States; governing judicial rulings; and the Immigration and Nationality Act, Section 287(a) (8 U.S.C. Section 1357). The principal court case that affirmed Border Patrol authority to conduct traffic checkpoints was *U.S.* v. *Martinez-Fuerte*, 428 U.S. 543, 556 (1976).[1]

Border Patrol traffic checkpoints, such as the proposed permanent facility on Interstate 91, are a critical component of CBP's multilayered border security strategy. The Border Patrol maintains over 50 such traffic checkpoints nationwide. Traffic checkpoints have been established to restrict the criminal elements' ability to use our highway system to further their entry into the United States. In addition, enforcement operations around the checkpoints target those attempting to avoid inspection by circumventing the checkpoints themselves, further enhancing homeland security. CBP has had discussions regarding the integration frequent traveler technology like NEXUS and PALS into the design of the permanent Interstate 91 checkpoint to ensure that regular highway users are impacted to the minimum extent possible.

The Border Patrol does not condone racial profiling, in fact during basic training Agents are instructed on how to perform their duties without profiling certain classes of people. Any and all allegations of racial profiling are taken seriously and are reported to the Office of Inspector General for investigation.

LAW ENFORCEMENT SUPPORT CENTER

Question. In your testimony, you mention that the Law Enforcement Support Center's workload increased by 12 percent last year. A number of the employees who are making this increase in productivity possible are temporary employees who have worked for the LESC for up to 4 years, with the expectation they would have the opportunity to become permanent employees. What are your plans to convert these temporary employees to permanent positions?

Answer. Law Enforcement Technicians (LETs) serving under term appointments have contributed significantly to the overall success of the ICE Law Enforcement Support Center (LESC). ICE recognizes that the workload of the LESC is a permanent one and shares the view that the staff should be permanent as well. It has been the practice of the LESC to convert term appointments to career appointments as permanent vacancies become available. It has also been the practice of the LESC to regularly extend term appointments up to their maximum duration. However, LESC term LETs are serving under term appointments that have a maximum duration of 4 years under Federal personnel rules and cannot be further extended. The majority of LETs serving under term appointments will not reach their 4-year limit until the spring and summer of calendar year 2006. Only one will reach the 4-year limit in calendar year 2005. The remainder will not reach their 4-year limit until calendar year 2007. As term appointments approach their expiration dates, ICE will explore all available options consistent with Federal personnel rules, budgetary considerations and good management to retain these valuable employees.

DEBT MANAGEMENT CENTER

Question. The ICE Debt Management Center is an integral part of the financial stability of the bureau. Responsible for collecting debts owed to the agency, the center is an important part of balancing the books at ICE. Has the bureau wide hiring

[1] Additional case law references: *U.S.* v. *Gordo-Marin*, 497 F.Supp. 432 (S.D Fla. 1980), and *U.S.* v. *Maxwell*, 565 F.2d 596 (9th Cir. 1977).

freeze affected the ability of this debt management center and all other financial offices perform their duties? Have you considered providing some flexibility from the hiring freeze for offices with financial responsibilities? As these offices loose individuals from normal attrition, it seems ironic that the offices with responsibilities to correct the financial situation

Answer. As with all of ICE Financial Management operations, the Debt Management Center is committed to fully addressing all of its financial management responsibilities in a timely manner. If approved by Congress, the ICE reprogramming proposal will provide additional support to the Debt Management Center (DMC), and the DMC, along with ICE's Office of Financial Management is closely monitoring ongoing operations to ensure that essential and critical financial management requirements are completed in a timely manner.

The ICE OFM has gone through a re-engineering process, finalized in December 2004. The re-engineering format allows the OFM to address audit and financial statement activities (abnormal balances, suspense, cash reconciliation, trading partners, reconciliation of unliquidated obligations, and analysis) as well as specific financial transactional activities for our customer base (Debt Management Center, Dallas Finance Center, financial system support of FFMS and Travel services).

LEGAL ORIENTATION PROGRAMS

Question. I have supported and helped to obtain funding for Legal Orientation Programs for immigration detainees, with the view that the immigration system works better for all parties when detained aliens are informed as to whether they have a legitimate legal case to stay in the United States. Congress appropriated $1 million for orientation proceedings in fiscal year 2003, but DHS has still not transferred that money to the Executive Office for Immigration Review so the proceedings can take place. Can you tell me when that money will be transferred, and why it has taken so long?

Answer. ICE has provided $3 million to the Executive Office of Immigration Review (EOIR) for the Legal Orientation Program covering services in fiscal year 2003 through fiscal year 2005. The funding was provided in increments of $1million at the following times:

$1 million to EOIR in late July 2002 (fiscal year 2002).

$1 million to EOIR in February 2004 (fiscal year 2004).

$1 million to EOIR in February 2005 (fiscal year 2005).

As indicated above, the first $1 million was issued very late in fiscal year 2002. EOIR used this fiscal year 2002 funding to award a contract for legal orientation program services that were provided throughout fiscal year 2003. EOIR continued to provide legal orientation services based on funding provided in February 2004, and currently provides legal orientation program services with an additional $1 million provided in February 2005. There have been no gaps in providing legal orientation program services because of lack of funding.

CITIZENSHIP AND IMMIGRATION SERVICES FUNDING

Question. The President's budget proposes a 50 percent cut in the amount of directly appropriated funds for the Bureau of Citizenship and Immigration Services (CIS), from $160 million to $80 million. Congress has already substantially cut the direct appropriations you receive. At the same time, the President has proposed a guest worker program that would significantly increase the CIS workload. (A) Why is the President proposing a 50 percent cut in an agency whose workload he wants to increase dramatically? (B) Are you at all concerned that a system of immigration services that is supported almost entirely by user fees—including the expansion of "premium processing" fees paid to ensure faster processing—will be unfair to immigrants of lesser means?

Answer. The fiscal year 2006 Budget includes $1.854 billion for USCIS ($80 million appropriated; $1.774 billion fees), an overall increase of $79 million, or 4 percent over the fiscal year 2005 level. The fiscal year 2006 Budget is the final year of the President's 5-year plan to achieve a 6-month cycle time standard for all immigration benefit applications, including a total of $100 million to support backlog elimination efforts as well as improvements in application processing. This would bring the 5-year total for this aggressive initiative to $560 million. Backlog elimination funds are reduced by a total of $80 million. $60 million associated with a one-time increase in the fiscal year 2005 USCIS budget, and $20 million for Digitization efforts appropriated by the Congress, but not specifically requested in the President's budget. The fiscal year 2006 Budget will allow USCIS to eliminate the backlog by the end of fiscal year 2006.

USCIS is committed to meeting the President's backlog elimination goals. The key to processing temporary worker petitions quickly and efficiently is simplicity in the design. Establishing a program that involves a high degree of employer/government partnership, thorough background checks, and electronic registration and information sharing among participating Departments is critical. Based upon the legislation that Congress passes, USCIS will use fees to support applicant registration, processing and documentation.

While Federal guidelines require full cost recovery of services provided, USCIS does have the ability to waive fees on a case-by-case basis. Any applicant or petitioner who has an "inability to pay" the fees may request a fee waiver. In determining "inability to pay," USCIS officers will consider all factors, circumstances, and evidence supplied by the applicant including age, disability, household income, and qualification within the past 180 days for a Federal means-tested benefit.

SUBCOMMITTEE RECESS

Senator COCHRAN. We are going to continue to review the budget request for fiscal year 2006 for the Department of Homeland Security. Our next hearing will be on Wednesday, March 9, in Room 124 of the Dirksen Senate Office Building. At that time the Under Secretary for Emergency Preparedness and Response, Mr. Michael Brown, and the Acting Director of the Office of State and Local Government Coordination and Preparedness, Mr. Matt Meyer, will be here to discuss the budget request for the programs under their jurisdictions.

Until then, the subcommittee stands in recess.

[Whereupon, at 12:23 p.m., Wednesday, March 2, the subcommittee was recessed, to reconvene subject to the call of the Chair.]

DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR FISCAL YEAR 2006

WEDNESDAY, APRIL 20, 2005

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10:30 a.m., in room SD–124, Dirksen Senate Office Building, Hon. Judd Gregg (chairman) presiding.

Present: Senators Gregg, Domenici, Craig, Allard, Byrd, Leahy, Kohl, Murray, and Feinstein.

DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF MICHAEL CHERTOFF, SECRETARY

OPENING STATEMENT OF SENATOR JUDD GREGG

Senator GREGG. I call the hearing to order.

Senator Byrd is the ranking member on this committee, and obviously on the full committee, and he will be here a little later. And when he arrives we will accord him the opportunity of making an opening statement if he should so wish.

We appreciate Secretary Chertoff coming here today. He's just assumed one of the priority responsibilities in our government relative to the safety of Americans. He's given up an extremely important position to take this position on, and it reflects well on him and I think on this administration as somebody who has caliber and is willing to do this type of a job, and we appreciate it.

However, the agency he takes over has some very serious problems, and this morning before this hearing I was just writing down—and I didn't do this with any staff assistance—just off the top of my head, the problems that I've seen and been reported to me over my brief tenure as chairman of this committee, they include things like the border patrol, the fact that our borders are not effectively protected anymore, that they are not—we have virtually no security along our borders, that people are pouring over the borders illegally.

It's gotten so bad that in Arizona citizen groups are now seeking to enforce the borders, which obviously is not good, that the border patrol training capabilities are not up to what the Congress asked them to be. We asked for 200 agents a year to be trained. Maybe they can do 400, 500, if they are fortunate. They cannot find people. They cannot hire them.

IMMIGRATION

In the area of immigration, this is an agency which has had a very long history of very significant management issues. Back when I chaired the Subcommittee on Commerce, State, and Justice before this Department was moved over to DHS; the Department had a lot of problems.

Even under the prior administration, the problems were significant and they have continued in the area of management. I don't think any member of Congress receives complaints about any agency with more consistency than about the immigration issues that we get.

IT ISSUES

We have got the issues of IT. The inability of the fingerprint capability at the borders to communicate effectively and in real-time with the database of the FBI. IDENT is not integrated into IAFIS.

We have the US VISIT program, which I have serious reservations about whether it is going where it is supposed to be going as a technology capability.

TSA

We have the TSA. It has become almost a weekly event now that there is some report that comes out about the TSA's failures in a variety of areas, from waste and fraud in the most recent IG report relative to the construction of its facilities for its headquarters to an internal investigation which I guess concluded that weapons and contraband were still going through the airports with regularity, which was totally unacceptable, to what I consider to be an inexcusable situation of a large amount of theft being reported from passengers in this country.

The fact that an agency of the Federal Government would have thousands upon thousands of reported thefts occurring by Federal employees against American citizens makes us look like a third-world country. And it still goes on.

Workman Compensation claims are outrageous. And I think anybody who goes through airport security has to ask themselves, at least occasionally when going through airport security, is this really having an effect on security or is this simply mindless when you see some of the actions taken by the TSA.

INTELLIGENCE

The intelligence issue, the agency has ceded intelligence over to other agencies when originally it was supposed to be the center of basically coordinating of intelligence. And now we see that the intelligence decisions are being made outside the agency by a conscious decision. And maybe it was the right decision, but essentially the IAIP has been raided the last 2 years from its resources to do other things. And I view intelligence as probably the essence of whether or not we win this war.

This is not a war about reacting to events. It is a war about getting to those events before they occur. And that involves intelligence.

PERSONNEL CONCERNS

The personnel issues, the senior management turnover is extraordinary. The number of people in an acting position is unacceptable and the number of positions which are unfilled at senior management levels is unacceptable.

ELECTRONIC SURVEILLANCE ALONG THE BORDER

The electronic surveillance capability along the border is non-existent right now from all I can tell. There has been a total breakdown in the camera structures; and the unmanned vehicle program has basically been stopped, even though it was proving very successful.

OTHER CONCERNS

Contingent to the agency's responsibility is the issue of protecting us against a biological or chemical attack. And granted, the HHS has priority here, but the Department has a very significant role in making sure that HHS is successful. And it is very obvious that in the area of vaccines, Bioshield has not produced the results it should have produced, and that we have not created a robust vaccine capability in this country against very significant disease issues, specifically anthrax, botulism, plague, and small pox.

Container ships, we all know we are not getting anywhere near the scrutiny on the container ships. If we look at the agency objectively, just on that list you have to say that were this agency admitted to an emergency room, it would be considered to be in extreme distress.

The fact is we have not been attacked. And credit on that goes to the Department, and I give them credit for that. But the fact also is there are very serious, serious problems, especially on what I consider to be the three core elements of the Homeland Security portfolio, which is protecting us from weapons of mass destruction attack, protecting our borders, and making sure that they are under control, and making sure that we have adequate intelligence capability.

So the problems exist now. You did not create them, Mr. Secretary. They did not come on your watch. You have just arrived. I congratulate you for setting up a Department-wide review of what is going on and trying to figure out how to correct it. But they exist and we have to get our arms around them.

FISCAL YEAR 2006 BUDGET REQUEST

The budget that has been sent up by this Administration presumes that the Congress will pass a significant increase on the fees of people who are flying. I do not think you are going to see this Congress accomplish that. Certainly, the chairman of the Commerce Committee here in the Senate has been more than vociferous in opposition to that proposal, and that is his authorizing committee, although this appropriating committee will play a role.

But if you take that number out, the budget that was sent up is well over a billion dollars less than last year's budget to operate this Department. If you put that number in, and giving you the benefit of the doubt that we are going to raise the fees on travelers

in this country by dramatic amounts, even though the stated amount is that the budget is up by 7 percent, our estimate is that the budget is up by about a $100 million.

Now it may not be that money solves this problem. In fact, I do not think it does. I think a lot of this is an issue of management and structure. But we know, for example, in the area of border patrol that getting more bodies on the border is critical, and that is going to cost money. And there are other areas where we know money may make a difference, for example, backlogs.

So I am not sure the budget that has been sent up is reflective of the urgency of the problem that this Department has relative to different functions that in my opinion are in distress.

So I hate to start this hearing off with a dark cloud, but I think honesty is required, and these are not reports which I have manufactured. They are restatements of public information.

So with that, again, I want to emphasize that I feel that we are extremely fortunate that you have been willing to take this job on. But I think you have been dealt a hand that is difficult to play, and I am looking forward to working with you to try to improve that hand. And that is the purpose of this committee, to constructively work with you to give you the resources you need to accomplish the improvements so that a year from now we do not have this long list of concerns. With that, we will listen to your thoughts.

STATEMENT OF MICHAEL CHERTOFF

Secretary CHERTOFF. Well, thank you, Mr. Chairman. And thank you for welcoming me to this first appearance for this subcommittee, which I am looking forward to working with as we go forward to improve our performance and make sure we are on the right track to, as you point out, protecting the American people, and protecting our infrastructure. And then if worse comes to worse, appropriately responding.

If I may, I would like to ask that the subcommittee receive my full statement for the record.

Senator GREGG. Of course.

Secretary CHERTOFF. I am going to be very brief so that I can be available to answer questions. Let me try in just a couple of moments to give you at high altitude the approach that I think we are taking in this review we have got going, and also in terms of our moving forward with the Department.

Quite obviously, in creating the Department, Congress wanted to do more than assemble 22 organizations in a tent. We wanted to create a single organization that could achieve outcomes that are important in terms of enhancing our national security. So one of the critical tasks I think I have as I begin my tenure at the Department is to see what we need to do in order to further the process of integration.

I completely agree that means intelligence, which is the driving guide to what we do all across the board. And we need to make sure we are appropriately collecting and fusing the intelligence we have available within the Department, and then contributing that to the community at large and consuming what the community has, and operationalizing that.

So we are looking to enhance our ability across the Department to combine our intelligence, combine our operations, and combine our policymaking. So we have a Department-wide approach to these things.

Second, as part of the review we are undertaking, I really want to be focused on outcome, and to kind of boil the jargon away. The example I have given to people when I try to explain what I mean, if my car is not running and I take it into the shop, and the electrician and the guy who does the transmission and everybody else takes a whack at it, and I come in at the end of the day to pick the car up, and everybody says, wow, you know, we have each done our process exactly right, but the car does not run, I do not consider myself a satisfied customer.

I am concerned about the outcome. I want a car that runs. And that is true here, too. We want a Department that produces the outcomes we care about, and we ought to focus on how we do that without regard to everybody's individual stove pipes. And then the alignment of the stove pipes and the alignment of the organizations and the operations has to be what fits with getting the outcomes.

The third piece is, we do want to use this risk-management philosophy. I think you pointed out, Mr. Chairman, in your statement, there are a lot of important things, but there are some things that are the highest priority. WMD is one example. And we have to be disciplined, since we are talking about a long-term issue with terrorism and threat, about identifying the priorities and figuring out how we go about optimally taking what are obviously finite resources and getting them to where they have to be. And so that risk management approach is going to be our guiding philosophy.

We are not interested in the Department of Homeland Security as simply an opportunity for people to, you know, raid the pots of money. We are interested in making sure that we get the money and everything we do over our deployment and our operations in a risk management, focused manner.

PREPARED STATEMENT

So with these kind of general observations, again, I am delighted to work with the subcommittee. I know it is a very challenging position, but I know there is a tremendous amount of support with the American public to getting this job done right. And that is what I am going to do my level best to do, and I look forward to answering questions.

Senator GREGG. Thank you. Thank you, Mr. Secretary.

[The statement follows:]

PREPARED STATEMENT OF MICHAEL CHERTOFF

INTRODUCTION

Mr. Chairman, Senator Byrd, and Members of the Subcommittee: Thank you for the opportunity to address you today, and for your ongoing support of the Department of Homeland Security's efforts to keep America secure and free. I am honored and pleased to appear before the Senate Appropriations Committee, Subcommittee on Homeland Security. This is my first appearance before this Subcommittee, and I look forward to a productive exchange as the Department begins to reassess and readjust priorities and policies in accordance with the changing threat of terrorism over three and a half years after the September 11, 2001 attacks.

For more than 2 years now, the Department of Homeland Security has led a national effort to protect our country and our citizens from all manner of threats. It has been an honor to join the dedicated men and women who carry out this task daily. Ours is a difficult mission—to prevent another deadly and catastrophic terrorist attack such as the one we experienced on September 11, and if an attack occurs, to respond quickly and prevent further damage.

The 180,000-plus people of the Department carry out this mission with unflinching resolve and a driving determination that such an attack should never occur on American soil again. Realizing that we can make no guarantees, we pursue our mission with a sense of urgency and daily diligence, so that this Nation can respond and recover quickly, should an incident or attack occur.

Since its establishment just over 2 years ago, DHS has made great strides in its efforts to unify the defense of our homeland. We have continued to integrate 22 distinct agencies and bureaus, each with its own employees, mission and culture.

But our security requires even greater coordination and effort throughout the Department, across all levels of government, and throughout our Nation to create synergy and new capabilities. It requires an unwillingness to accept complacency as part of anything we do; rather, we know we must apply all effort to tear down stovepipes and coordinate key intelligence, policy, and operational issues across DHS and the government.

SECOND STAGE REVIEW

I have therefore initiated a comprehensive review of the organization, operations and policies of the Department as a whole. This comprehensive review will examine what we are doing and what we need to do without regard to component structures and programmatic categories.

We want to understand better what's working and what isn't. We will be evaluating every element of our working mission and making sure that the Department is best organized to meet the threats—both current and future—that face our Nation.

Old categories, old jurisdictions, old turf will not define our objectives or the measure of our achievements because bureaucratic structures and categories exist to serve our mission, not to drive it.

Deputy Secretary Michael Jackson has been charged with overseeing this process. The goal of the review is to help me make informed decisions as I lead the Department. Deputy Secretary Jackson has selected a team of Department officials to look at a number of critical cross-cutting issues and determine how departmental resources and programs can be most effectively applied to achieve our security goals. I have asked them to get back to me by Memorial Day with the bulk of their recommendations. I intend to study and act on their recommendations.

What will the review cover? Take an issue such as maritime cargo security, which cuts across several departmental components. Customs and Border Protection, Coast Guard, Science and Technology, and Information Analysis and Infrastructure Protection each address aspects of this overall mission. Each might perform its element well, but we must go further to ensure that each is performing seamlessly and in coordination with the others, that we eliminate any duplication of effort, and that we reap the full strength of our wide spectrum of capabilities.

Of course, in executing the initial phase of putting the Department together and integrating the different components into a working structure, my predecessor and the men and women of Homeland Security did a tremendous job. They should be commended.

Now, as we enter into the second phase of the Department's life, we must also take a fresh, creative look at the Department itself—including its organization, its operations, and its policies. We are not yet fully integrated and our entities are still not always coordinated with each other. Now the challenge is to take the advantage of 2 years' experience and evaluate the Department to see if there are potential structural and operational changes that will improve and enhance our capabilities to protect and safeguard this Nation.

CROSS-CUTTING FUNCTIONS AND INTEGRATION

On the most basic level, we need to take a step back and focus on the fundamental question: Why was the Department of Homeland Security created? It was not created merely to bring together different agencies under a single tent. It was created to enable these agencies to secure the homeland through joint, coordinated action. Our challenge is to realize that goal to the greatest extent possible.

Let me tell you about three areas where I plan to focus our efforts to achieve that goal. First, we need to operate under a common picture of the threats that we are

facing. Second, we need to respond actively to these threats with the appropriate policies. Third, we need to execute our various component operations in a unified manner so that when we assess the intelligence and we have decided upon the proper policies, we can carry out our mission in a way that is coordinated across the board.

My intent is to integrate each of these three areas—intelligence, policy, and operations—across the Department, so that each is directed from the most senior level of the Department.

Let me turn to intelligence. Intelligence plays a pivotal role in mapping our mission. When the Department was created, 22 separate and distinct entities were woven together, a number of which had components focused on intelligence-gathering and analysis. One of my top priorities is to make sure that these various intelligence components function as a cohesive unit, and that our information and analysis is coordinated across the Department so that DHS, as a full member, can enhance its contribution to the Intelligence Community.

First, we must organize and combine all intelligence within DHS. To do this effectively, we must ensure that our own intelligence components are interoperable. The Department has already made progress in this area. For example, the Homeland Security Operations Center was stood up to help the Department develop a common operating picture and facilitate information sharing.

We must make sure that we are gathering all relevant information from the field, communicating with each other, and approaching analysis with a mission-oriented focus. We must ask, for example, whether those who evaluate the border from the Customs and Border Protection perspective are learning from analysts in the U.S. Coast Guard. They each look at border security, but from different vantage points. Only if they are working together can they fill in key gaps, paint a realistic picture, and evaluate all of the different pieces of information and intelligence that they are each gathering. We have to maximize the fact that all of these components now exist under the same umbrella.

Second, we must make sure that information is being disseminated both up and down the ranks of the Department. Strong and effective coordination does not just mean that our analysts at DHS headquarters are working together. We need to fuse and exploit all the information that we learn across the country, so that when a Border Patrol agent in Texas learns of a new alien smuggling method, that information is fed up to our intelligence analysts, incorporated where appropriate into our strategy to combat smuggling, and disseminated across the Department to others focused on the same problem. We must build a culture in which the disparate pieces of information are being transmitted to our analysts so that they, who have the benefit of the fuller picture, can properly analyze all of our information and inform our decision-making.

The converse must be true when our intelligence analysts learn of new vulnerabilities that terrorists are trying to exploit. That same agent in Texas needs to know, on a timely basis, of the threat and what he should be looking out for. We have a great many talented individuals at the Department. Some gather and analyze intelligence. Others learn critical information as they are in the field performing their jobs. The opportunities are endless. DHS needs to bring all of these nuggets of information together and disseminate them appropriately. We need to have the structure and the correct systems and technologies in place to take full advantage of them.

Third, our focus must extend beyond the Department itself. We must review and make use of intelligence coming from the Intelligence Community and we must play an active role in providing intelligence information to the Intelligence Community. As the WMD Commission made clear in its report 2 weeks ago, sharing information across the Federal Government is critical if we are to succeed. To that end, I am committed to making sure that our law enforcement and intelligence partners across the Federal Government have appropriate access to the Department's information and analysis, to the maximum extent possible under the law, while protecting the privacy rights and civil liberties of Americans. By the same token, we must sit as full partners at the table with full access to others in the Intelligence Community. We must work in concert with the Intelligence Community. I will work closely with the Director of National Intelligence, whose job it will be to make sure that the Intelligence Community is well-coordinated and mission-focused.

In addition, intelligence and information from other Federal agencies is critical to our efforts to secure the homeland. The development of the terrorism information sharing environment, as called for under the Intelligence Reform and Terrorism Prevention Act, will connect the resources (people, systems, databases, and information) of Federal, State, and local governments, and the private sector allowing users to share information and improve collaboration.

Finally, we must inform and communicate with our State, local, tribal entities, and private sector partners. As I observed just last week during TOPOFF, when it comes to securing the Nation, we must ensure that these entities are well-equipped both to react to crisis and to prevent it. As part of this effort, we must improve our ability to operationalize intelligence. As information comes in, we need to make sure it is getting out to the right people and in a way that they can use to strengthen their efforts and contribute effectively to ours. Intelligence in a vacuum is meaningless. We need to explain how our outside partners can counter that threat and what we need them to do to watch out for it.

Now, let me address policy development. Development and coordination of policy are major responsibilities of this Department. The Department has the central mission of securing the homeland, but there are many different aspects of that mission with numerous contributors. Large elements of DHS include traditional operational functions in which we deploy personnel, equipment, planes, ships and vehicles. But other elements principally involve planning and rule making, and networking with State, local, and tribal entities, and private parties. All of these must serve and promote our homeland security imperatives.

Therefore, we need to further enhance our capability to think through broad and overarching issues like border security, emergency preparedness, transportation security, and cargo security, with a Department-wide perspective, rather than just through the lenses of one particular component. We need to develop our policies by first looking at our missions and asking the comprehensive, result-oriented questions, rather than by looking to one particular entity that has the lead in driving an issue to conclusion.

Accordingly, I believe that we should pull together the vast expertise and the varying perspectives already at the Department as we work toward integrating our many crosscutting functions. For this reason, one of the areas that we are closely studying in the Second Stage Review is the advisability of creating a department-wide, substantial policy office. This office will also be a very important focal point for coordinating DHS's policy work with other Federal, State, local, and tribal entities.

Finally, let me discuss operational coordination. Just as with intelligence and policy, we need to find new ways to increase our operational coordination. Diverse operational components were woven together when Congress stood up the Department, each with its own history and identity. As I have become acquainted with these various components, I have quickly learned that there is a great deal of talent within them. Each entity has its own unique focus, but often they address the same mission from differing perspectives. But we cannot function as a cohesive unit, unless each operational component works together in combination to promote common missions.

This means that our operations must be driven by mission-oriented plans. It can no longer be the case that different components tackle different problems each in its own way and then later look to see if the pieces fit together. Whether it is preventing a potential act of terrorism, emergency preparedness, border protection, or countering a particular threat, we must first define the mission and second deploy all the tools within the Department to effectively execute each operation.

The Department has already begun this process. To take but one example, on the Arizona border, we have a cross-cutting initiative to protect the border, integrating intelligence gathering, border enforcement, and monitoring. It encompasses the efforts of several of our agencies, including Customs and Border Protection, Immigration and Customs Enforcement, Science and Technology, the Coast Guard, and Information Analysis and Infrastructure Protection. Each plays an integral role. The operations themselves involve patrolling the border, generating information, and using it to take enforcement actions. The genius of the Department of Homeland Security is that we have the capability within one department to do all of these things. But we need to carry out joint operational activities and have a joint perspective on a routine basis, not only when we stand up a special project.

Operations are also the mechanisms by which we respond to crisis. We cannot wait for a crisis, however, to learn, for example, whether TSA has the capability to communicate effectively and coordinate with FEMA. Nor can we learn in crisis that both are conducting the same operations or sending different messages to the private sector. The Department has made significant progress in this area. For example, it developed the National Response Plan to more effectively map out how to handle crisis situations. Now is the time to organize around missions rather than old bureaucracies, work through all of these potential disconnects in our systems, and operate as one unified Department. But integrating ourselves cohesively is not enough.

RISK-BASED APPROACH

I have been saying, and you will continue to hear me say, that we need to adopt a riskbased approach in both our operations and our philosophy. America is dynamic. Our strength as Americans is the sum of every generation that has ever been born in or immigrated to this great land. Our wealth and livelihoods are advanced by the inspired ideas and innovation of our own people. We prosper through the vast opportunities that exist to interact with the global economic community.

Risk management is fundamental to managing the threat, while retaining our quality of life and living in freedom. Risk management must guide our decision-making as we examine how we can best organize to prevent, respond and recover from an attack. We need to be realistic in our prioritization. We must assess the full spectrum of threats and vulnerabilities.

We all live with a certain amount of risk. That means that we tolerate that something bad can happen; we adjust our lives based on probability; and we take reasonable precautions. So, too, we must manage risk at the homeland security level. That means developing plans and allocating resources in a way that balances security and freedom when calculating risks and implementing protections.

The most effective way, I believe, to apply this risk-based approach is by using the trio of threat, vulnerability, and consequence as a general model for assessing risk and deciding on the protective measures we undertake.

Here I inject a note of caution because the media and the public often focus principally on threats. Threats are important, but they should not be automatic instigators of action. A terrorist attack on the two-lane bridge down the street from my house is bad but has a relatively low consequence compared, to an attack on a major metropolitan multi-lane bridge. At the other end of the spectrum, even a remote threat to detonate a nuclear bomb is a high-level priority because of the catastrophic effect.

Each threat must be weighed, therefore, along with consequence and vulnerabilities. As consequence increases, we respond according to the nature and credibility of the threat and any existing state of vulnerabilities. Our strategy is, in essence, to manage risk in terms of these three variables—threat, vulnerability, consequence. We seek to prioritize according to these variables . . . to fashion a series of preventive and protective steps that increase security at multiple levels. We must examine the mission and work of all elements of DHS through this template of consequence, vulnerability and threat. Have we fully defined our missions? How far have we gone in carrying them out? What more needs to be done?

The Department is already working with State, local, and private sector partners to further refine the Interim National Preparedness Goal to aid the targeting of resources to where the risk is greatest. There is much that we are doing. DHS agencies, for example, have provided unprecedented level of funding and resources since 9/11 to State, local and private sector partners to protect and prepare America's communities and individual citizens. We continue to improve the ways for first responders across the Nation to be better equipped, better trained and more capable of communicating across the public safety community. But we must bring even greater focus and discipline to our preparedness mission. We need to take a very substantive look at how we align our preparedness activities and functions. We need to look at how best to configure our organizations, operations, programs and policies so that we can think strategically about preparedness.

What should drive our intelligence, policies, operations, and preparedness plans and the way we are organized is the strategic matrix of threat, vulnerability and consequence. And so, we'll be looking at everything through that prism and adjusting structure, operations and policies to execute this strategy.

FISCAL YEAR 2005 ACCOMPLISHMENTS

Before beginning to outline the major themes of the Department's fiscal year 2006 Budget request, I would like to highlight a few of the Department's accomplishments over the past year, including the following:

—The Department established "the One-Stop-Shop" for first responder grants which allows a single point of entry to the Federal Government for homeland security preparedness resources.

—DHS has provided unprecedented levels of funding and resources to State, local and private sector partners to protect and prepare America's communities and individual citizens. We continue to improve ways for first responders across the Nation to be better equipped, better trained and more capable of communicating across the public safety community.

—U.S. Citizenship & Immigration Services (USCIS) is on track to eliminate the backlog of immigration benefit applications by the end of fiscal year 2006. In

fiscal year 2004, the agency increased productivity by 21 percent and successfully reduced the backlog to 1.3 million cases—down from a high of 3.8 million cases in January 2004.

—United States-Visitor and Immigrant Status Indicator Technology (US VISIT) was successfully implemented at 115 U.S. international airports and 14 seaports and immediately demonstrated results by preventing individuals with criminal records and immigration violations from entering the United States. In addition, US VISIT successfully deployed initial capability to the 50 busiest land border ports of entry in December 2004 and was also deployed at pre-clearance airports in Canada, Bermuda, the Caribbean and Guam.

—The U.S. Coast Guard (USCG) developed, reviewed, and approved 9,000 domestic vessel security plans; 3,200 domestic facility plans; 48 Area Maritime Security Plans and Committees; and verified security plan implementation on 8,100 foreign vessels.

—USCG interdicted nearly 11,000 undocumented migrants attempting to enter the country illegally by sea, saved the lives of nearly 5,500 mariners in distress and responded to more than 32,000 calls for rescue assistance.

—Counterdrug efforts remain a top priority for the Department. With the passage of the December 2004 Intelligence and Reform Bill, the Department's Office of Counternarcotics Enforcement is heavily invested in ensuring counterdrug operations and policy are synchronized across the Department, and that our components are adequately resourced to perform their counterdrug mission. In fiscal year 2004, the Coast Guard, Immigration and Customs Enforcement, and Customs and Border Protection collectively kept 489,870 pounds of cocaine from reaching the streets of our Nation.

—In support of Operation Iraqi Freedom the USCG protected, safely secured, and escorted to sea over 200 military sealift departures at ten different major U.S. seaports, carrying over 25 million square feet of indispensable cargo.

—The Homeland Security Operations Center (HSOC) Homeland Security Information Network (HSIN) infrastructure to facilitate providing Secret level connectivity has been expanded to state level Emergency Operations Centers in all 50 States, territories, and the District of Columbia.

—The Department's Information Sharing and Collaboration Office (ISCO) is responsible for producing immediate, near-term and long-term improved information sharing processes and systems. ISCO successfully partnered with DOJ to establish a first ever capability to share information between systems supporting law enforcement users across the country. The Homeland Security Information Network (HSIN), Regional Information Sharing System (RISS), Law Enforcement On-line (LEO), and Criminal Information Sharing Alliance Network (CISANet) now share information posted on each system with the users of the other systems with the result that over 7,000 documents are already posted and the numbers are growing every day. Users are able to access information on any of the four systems through a single sign-on, thus eliminating the need to access all four network simultaneously.

—Working closely with importers, carriers, brokers, freight forwarders and others, Customs and Border Protection (CBP) has developed the Customs-Trade Partnership Against Terrorism (C–TPAT) program, which has become the largest government/private partnership to arise from September 11.

—In carrying out its agricultural mission, Customs and Border Protection (CBP) Agricultural Specialist conducted 3,559,403 cargo inspections, 111,416,656 passenger inspections and made more than 400,000 interceptions of prohibited meat and animal by-products. During the same time period, CBP agricultural specialists intercepted more than 96,000 prohibited plant materials and found more than 64,000 agricultural pests.

—The Federal Emergency Management Agency (FEMA) provided $4.9 billion in aid, including hurricane relief efforts for victims and communities affected by disasters. FEMA, with its DHS counterparts, responded to 65 major disaster declarations and seven emergencies in fiscal year 2004.

—Passenger screening by the Transportation Security Administration (TSA) kept 6,501,193 prohibited items from coming on board aircraft during fiscal year 2004.

—In 2004, TSA screened approximately 600 million checked bags using advanced explosive detection technologies and over 31 million mail parcels using explosive detection canine teams.

—Since establishment of the Federal Flight Deck Officer (FFDO) Program in February 2003, TSA has selected, trained, and armed thousands of volunteer flight crewmembers to defend the flight decks of commercial passenger and cargo aircraft against acts of criminal violence or air piracy. To date, hundreds of thou-

sands of flights have been protected by one or more FFDOs serving in mission status.

—A total of 428 million people, including 262 million aliens, were processed at land, air and sea ports of entry. Of that number 643,000 aliens were deemed inadmissible under U.S. law.

—Immigration and Customs Enforcement (ICE) officers achieved a 112 percent increase over the prior year for fugitive apprehensions resulting in more than 7,200 arrests. ICE removed more than 150,000 aliens in 2004.

—Border Patrol agents apprehended almost 1.2 million illegal aliens between our official ports of entry.

—The Container Security Initiative (CSI), which involves pre-screening shipping containers to detect and interdict terrorists' weapons and other illegal material, was expanded to include 21 countries. CSI is now operational in 34 foreign ports in Europe, Asia, and Africa.

—Approximately 600 million checked bags were screened using advanced explosive technologies in 2004.

—More than 2,500 criminal investigations were conducted involving the illegal export of U.S. arms and strategic technology, including Weapons of Mass Destruction (WMD).

—The Federal Law Enforcement Training Center (FLETC) provided basic and advanced law enforcement training to more than 44,750 students, representing 81 Federal agencies, as well as State, local and international law enforcement organizations.

—Border and Transportation Security (BTS) assumed responsibility for visa policy under the Homeland Security Act and implemented improvements in visa review times and transparency.

—The Department planned, designed, and implemented security for five events designated as National Security Special Events (State of Union Address, G–8 Economic Summit, Former President Ronald Reagan Funeral, Democratic National Convention and Republican National Convention) as well as the support, integration, and coordination of hundreds of national special events not meeting the National Security Special Events designation.

—USSS arrested 30 individuals involved in global cyber organized crime, domestically and internationally. Industry experts estimate that $1 billion in total fraud loss was prevented.

—The Science and Technology (S&T) Directorate has implemented initiatives in chemical, biological, radiological, nuclear, and explosive (CBRNE) countermeasures, cargo security, border and transportation security, interoperability, standards for emergency responders, and cyber security. These initiatives have resulted in improved security of U.S. borders, transportation systems and critical infrastructure, and resulted in the greater preparedness of our Nation. To date, Department officials have visited more than 200 chemical, petrochemical, water, energy, (i.e. electricity, oil, liquefied natural gas, pipelines, storage, etc.) agriculture, commercial assets, national icons, soft targets, and mass transportation centers.

—The Department established the National Cyber Response Coordination Group (NCRCG) in partnership with the Department of Justice and the Department of Defense, as a forum of 13 principal agencies that coordinate intra-governmental and public/private preparedness operations to respond to and recover from largescale cyber attacks.

—The Department co-sponsored Blue Cascades II and Purple Crescent II, two regional tabletop cyber exercises in Seattle, WA and New Orleans, LA. Each exercise brought together more than 200 government and private sector officials to examine cyber security readiness and response procedures, highlight the importance of cyber security in critical infrastructure protection, and discuss solutions for integrating physical security and cyber security. Region-specific coordination and communication plans between first responders, the Federal Government, and critical infrastructure owners/operators were exercised.

—The Department established the US–CERT Control Systems Center to bring together government, industry, and academia to reduce vulnerabilities, respond to threats, and foster public/private collaboration to improve the security of the data and process control systems that operate our Nation's critical infrastructures.

—The Department established the Control Systems Security and Test Center (CSSTC) in conjunction with Idaho National Environmental and Engineering Laboratory, to provide an opportunity for government and industry to collaborate on cyber vulnerability enumeration and reduction activities for control systems currently in use across critical infrastructure sectors. The CSSTC models

map the cause and effect relationships of cyber attacks on control systems, assess the outcomes of actual events in a simulated environment, and provide the US–CERT with response and mitigation actions to share with partners in the control systems community.

—DHS and the Germany Ministry of the Interior jointly hosted a Multilateral Cyber Security Conference in Berlin, Germany. The conference brought together cyber security policymakers, managers from computer security incident response teams with national responsibility, and law enforcement representatives responsible for cyber crime from 15 countries. The conference program included a facilitated tabletop exercise and interactive discussions on how to develop an international framework—as well as near term actionable steps—for watch, warning, and incident response.

—The Information Analysis and Infrastructure Protection (IAIP) Directorate has developed and disseminated warning products (i.e. warning messages) to Federal, State, territorial, tribal, local, private sector, and international partners to protect citizens, governments, critical infrastructure, and key assets.

—IAIP has produced more than 70 "Common Vulnerability" reports executed over 250 Site Assistance Visits, nearly 600 Buffer Zone Protection Plans, and is continuing to build the National Asset Database. As of today, more than 80,000 "assets" have been compiled.

—Uninterrupted communications are critical for national security and emergency preparedness personnel in responding to a crisis. The National Communications System (NCS) issued an additional 17,000 calling cards, further enabling priority wire line phone communications and an additional 8,000 cell phones for priority wireless communications. In past disasters and crises, these capabilities have proved crucial.

—Pursuant to Homeland Security Presidential Directive-7, IAIP is coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States and has distributed the Interim National Infrastructure Protection Plan (Interim NIPP) to other Federal departments and agencies, the State Homeland Security Advisors, and the private sector stakeholder groups (e.g., the Homeland Security Advisory Council, Sector Coordinating Council, ISAC Councils, National Infrastructure Advisory Council, the U.S. Chamber of Commerce, etc.) The Interim NIPP provides a risk management framework for integrating and coordinating the Nation's infrastructure protection activities that takes into account threats, vulnerabilities, and consequences to manage a broad range of risks across the Nation's 17 critical infrastructure sectors.

—These important DHS activities were analyzed where appropriate for their impacts on personal privacy and civil liberties.

FISCAL YEAR 2006 BUDGET REQUEST

The Department's fiscal year 2006 Budget request revolves around five major themes: Revolutionizing the Borders; Strengthening Law Enforcement; Improving National Preparedness and Response; Leveraging Technology; and Creating a 21st Century Department.

REVOLUTIONIZING THE BORDERS

September 11, 2001 demonstrated the sobering reality that the United States is no longer immune from catastrophic attack. No longer do vast oceans and friendly neighbors provide the buffer against aggressive adversaries. In order to maximize the security of our Nation against persons determined to undermine the economy of the United States, our way of life and the freedoms we enjoy, the Department is determined to deter, thwart, and remove any threat to the Nation long before it reaches our borders. During fiscal year 2005, we will continue to strengthen our border security. For fiscal year 2006, the President's Budget includes several initiatives aimed at revolutionizing the Borders.

Weapons of Mass Destruction (WMD) Detection Technology is an integral part of the Domestic Nuclear Detection Office (DNDO) that includes a comprehensive strategy to address the threat of nuclear and radiological terrorism. The Budget includes $125 million to purchase additional Radiation Portal Monitors (RPMs) and pilot advanced next generation RPMs to detect both gamma and neutron radiation at our borders. In addition, the Container Security Initiative (CSI), which focuses on prescreening cargo before it reaches our shores, will have a preventative and deterrent effect on the use of global containerized shipping of WMD and other terrorist equipment. Egypt, Chile, India, the Philippines, Venezuela, the Bahamas and Honduras have been identified as expansion locations for this initiative in fiscal year 2006. An

increase of $5.4 million over fiscal year 2005 is included in Customs and Border Protection (CBP) budget for CSI. The total amount in the President's Budget for CSI is $138.8 million.

CBP's America's Shield Initiative (ASI) enhances electronic surveillance capabilities along the Northern and Southern land borders of the United States by improving the sensor and video surveillance equipment deployed to guard against the entry of illegal aliens, terrorists, WMDs and contraband into the United States. The Budget includes $51.1 million for ASI, an increase of $19.8 million. With additional technology investments, the President's Budget proposes to increase Border Patrol staffing over current levels to backfill staff vacated along the Southwest border, as well as increase staffing levels assigned to coastal areas. Since September 11, 2001, some Border Patrol agents were shifted to the Northern border in order to increase the number of agents assigned there. An increase of 210 positions and $36.9 million is included in the Budget for the Border Patrol. This increases the number of Border Patrol Agents to 10,949.

The Customs Trade Partnership Against Terrorism (C–TPAT), which began in November 2001, is another essential cargo security effort. C–TPAT focuses on partnerships along the entire supply chain, from the factory floor to foreign vendors to land borders and seaports. The President's Budget includes an increase of $8.2 million for this effort, bringing total funding for C–TPAT to $54.3 million. These funds will be used to enhance our ability to conduct additional supply chain security validations.

In addition to enhancing secure trade programs, the President's Budget also seeks to support additional investments in CBP's National Targeting System. CBP Targeting Systems aid in identifying high-risk cargo and passengers. The Budget includes a total of $28.3 million for these system initiatives, of which $5.4 million is an increase over the fiscal year 2005 level. Further, US VISIT, which will be consolidated within the Screening Coordination Office, will increase from $340 million to $390 million in the Budget. The increase will provide for the accelerated deployment of US VISIT at the land border and enhanced access for border personnel to immigration, criminal and terrorist information.

The President's 2006 Budget includes $966 million for the Integrated Deepwater System (IDS) to help address the Coast Guard's declining readiness trends and to transform the Coast Guard with enhanced capabilities to meet current and future mandates through system-wide recapitalization and modernization of Coast Guard cutters, aircraft, and associated sub-systems. Among other things, the IDS request funds production of the third Maritime Security Cutter-Large and continues HH–65 helicopter re-engineering to eliminate safety and reliability issues in the Coast Guard's operational fleet of short range helicopters.

Finally, within CBP, Long Range Radar technology is used by the Office of Air and Marine Operations to detect and intercept aircraft attempting to avoid detection while entering the U.S. CBP and the Department of Defense will assume responsibility for operating and maintaining these systems from the Federal Aviation Administration (FAA) beginning in fiscal year 2006. CBP's share is $44.2 million in the Budget.

STRENGTHENING LAW ENFORCEMENT

Law enforcement is a critical element in preventing terrorism across the Nation. Whether at the Federal, State, or local level, law enforcement agencies perform this vigilant task. As we know from unfortunate first hand experience, the known threats are creative, clever, and sophisticated. The Department's law enforcement agencies need to stay ahead of the threat. To achieve this, the Budget includes funding for numerous key initiatives to maintain and strengthen current law enforcement initiatives both within and beyond our borders.

The United States Coast Guard (USCG) is the Nation's leading maritime law enforcement agency. The President's Budget seeks additional investment in USCG assets to enhance its ability to carry out its mission. The President's budget provides $11 million to increase port presence and Liquefied Petroleum Natural Gas (LNG) transport security, funding additional Response Boat-Smalls and associated crews to increase presence for patrolling critical infrastructure, enforce security zones, and perform high interest vessel escorts in strategic ports throughout the Nation. This initiative also provides additional boat crews and screening personnel at key LNG hubs such as Baltimore, MD and Providence, RI to enhance LNG tanker and waterside security.

In addition, in the President's Budget, the Armed Helicopter for Homeland Security Project increases by $17.4 million. These funds will provide equipment and aircraft modifications to establish armed helicopter capability at five USCG Air Sta-

tions. This will provide the USCG and DHS with the tools needed to respond quickly and forcefully to emergency maritime threats. A total of $19.9 million is included in the Budget for this project. Finally, the Response Boat-Medium Project increases by $10 million the effort to replace the USCG's 41-foot utility boats and other large non-standard boats with assets more capable of meeting all of the USCG's multi-mission operational requirements. A total of $22 million is proposed in the Budget for this effort.

U.S. Immigration and Customs Enforcement (ICE), the largest investigative arm of the Department of Homeland Security (DHS), is responsible for identifying and shutting down vulnerabilities in the Nation's border, economic, transportation and infrastructure security. The President's Budget seeks a 13.5 percent budget increase for ICE, including increasing the Detention and Removal program by $176 million. For the Temporary Worker program, the Budget seeks to more than double the resources available for worksite enforcement including employer audits, investigations of possible violations and criminal case presentations. An increase of $18 million is proposed in the Budget for this effort. The President's Budget seeks a total of $688.9 million for ICE's Federal Air Marshal Service. This funding will allow ICE to protect air security and promote public confidence in our Nation's civil aviation system.

The Department's fiscal year 2006 Budget includes several other funding enhancements for law enforcement, including:

—The Federal Law Enforcement Training Center's (FLETC) budget increases by $2.7 million for Simulator Training Technology to teach officers and agents how to avoid collisions and reduce the dangers associated with pursuit driving.

—Federal Flight Deck Officers (FFDO)/Crew Member Self-Defense (CMSD) Training is increased by $11 million in fiscal year 2006. This allows for the expansion of the semi-annual firearm re-qualification program for FFDO personnel and to fund the first full year of the CMSD training program. A total of $36.3 million is included for FFDO/CMSD in the Budget.

—Enhancing law enforcement training through co-location of the Coast Guard's Maritime Law Enforcement Training program with the Federal Law Enforcement Training Center, increasing maritime law enforcement training throughput and promoting better coordination among field activities with other Federal, State, and local agencies.

IMPROVING NATIONAL PREPAREDNESS AND RESPONSE

Though the primary mission is to protect the Nation from terrorism, the Department's responsibilities are diverse. No DHS effort has a greater scope, reach and impact upon the citizens across the United States than our efforts to prepare the Nation to respond to major acts of terror or natural disaster. This Budget continues to support the President's homeland security directives that establish the methods and means by which our Nation prepares for and responds to critical incidents. Since its establishment, the Department has, and continues to provide, an unprecedented level of financial support to the State, local, and tribal governments and to certain private sector entities. The Budget builds on these efforts and proposes significant resources to provide direct financial assistance to our Nation's first responders, emergency managers, and citizen volunteers. There are several initiatives in the Budget geared towards improving national preparedness and response.

The fiscal year 2006 budget continues to support the Nation's first responders and seeks a total of $3.6 billion to support first-responder terrorism preparedness grants, administered by the Office of State and Local Government Coordination and Preparedness, with better targeting to high-threat areas facing the greatest risk and vulnerability. This funding will support State and local agencies as they equip, train, exercise, and assess preparedness for major emergencies, especially acts of terrorism. While there may be gaps in State and local capabilities, we believe special emphasis must be given to communications interoperability, catastrophic planning, WMD awareness, critical infrastructure protection, and cross-jurisdictional/regional cooperation and interaction.

For fiscal year 2006, the President's Budget proposes $20 million for the Federal Emergency Management Agency's (FEMA) enhanced catastrophic disaster planning. This funding will support catastrophic incident response and recovery planning and exercises. FEMA will work with States and localities, as well as other Federal agencies to develop and implement plans that will improve the ability of Federal, State, or local governments to respond to and to recover from catastrophic disasters quickly and effectively. FEMA will address the unique challenges a catastrophic disaster situation poses, including food and shelter, transportation, decontamination and long term housing needs.

On October 1, 2004, the Department of Homeland Security launched the Office of Interoperability and Compatibility designed to help State and local public safety practitioners improve communications interoperability. The Office of Interoperability and Compatibility (OIC), part of the Science & Technology directorate, oversees the wide range of public safety interoperability programs and efforts currently spread across Homeland Security. These programs address critical interoperability issues relating to public safety and emergency response, including communications, equipment, training, and other areas as needs are identified. The OIC allows the Department to expand its leadership role in interoperable communications that could be used by every first responder agency in the country. The OIC has currently identified three program areas: Communications, Equipment, and Training. With $20.5 million in fiscal year 2006, the OIC will plan and begin to establish the training and equipment programs, as well as continue existing communication interoperability efforts through the SAFECOM Program.

The President's fiscal year 2006 Budget for the Department proposes other enhancements to improve our national preparedness and response, including:

—Replacement of the USCG's High Frequency (HF) Communications System. Funded at $10 million in the Budget, this system will replace unserviceable, shore-side, high power high frequency transmitters, significantly improving longrange maritime safety and security communications.

—The Budget increases Cyber Security to enhance the U.S. Computer Emergency Preparedness Team (US–CERT), a 24/7 cyber threat watch, warning, and response capability that would identify emerging threats and vulnerabilities and coordinate responses to major cyber security incidents. An increase of $5 million is proposed, bringing the program total to $73.3 million.

—The Rescue 21 project is funded at $101 million in the Budget to continue recapitalizing the Coast Guard's coastal zone communications network. This funding will complete system infrastructure and network installations in 11 regions and begin development of regional designs for the remaining 14 regions.

LEVERAGING TECHNOLOGY

Rapid advances in technological capability are allowing the Department personnel to protect the homeland more efficiently and effectively across many components. To prepare the Nation to counter any WMD threat—threats from CBRNE substances—this Budget includes an increase for new initiatives that support research and development to counter these weapons and their potentially devastating effects.

First, the Domestic Nuclear Detection Office (DNDO) is being established as a joint national office to protect the Nation from radiological and nuclear threats. This office will consolidate functions within DHS and establish strong interagency linkages for the deployment of a national domestic nuclear detection architecture, the conduct of transformational research and development (R&D), and the establishment of protocols and training for the end users of equipment developed and deployed through the new office. The DNDO will integrate domestic nuclear detection efforts undertaken by individual Federal agencies, State and local governments, and the private sector and be closely linked with international nuclear detection efforts. A total of $227.3 million is requested for this effort in fiscal year 2006.

Second, TSA's emerging checkpoint technology is enhanced by $43.7 million in fiscal year 2006 to direct additional resources to improve checkpoint explosives screening. This request responds to the 9/11 Commission Report's finding that investments in technology may be the most powerful way to improve screening effectiveness and priority should be given to explosive detection at airport checkpoints for higher risk passengers immediately. This new equipment assures that TSA is on the cutting edge, ahead of the development of increasingly well-disguised prohibited items. This proposed increase will result in investing more than $100 million in fiscal year 2005 and fiscal year 2006 for new technology to ensure improved screening of all higher risk passengers.

In addition, to improve TSA's information technology network, the President's Budget includes $174 million to complete installation of High Speed Operational Connectivity (Hi–SOC) to passenger and baggage screening checkpoints to improve management of screening system performance. Within the Screening and Coordination Office, funding is sought for the Secure Flight and Crew Vetting programs—an increase of $49 million to field the system developed and tested in fiscal year 2005. The funds will support testing information systems, connectivity to airlines and screen systems and daily operations. This also includes an increase of $3.3 million for crew vetting.

Third, the President's Budget also proposes additional funding for two critical Department programs—the Homeland Secure Data Network (HSDN) and the Home-

land Security Operations Center (HSOC). For fiscal year 2006, the Budget includes $37 million for HSDN. This funding will streamline and modernize the classified data capabilities in order to facilitate high quality and high value classified data communication and collaboration. Funding for the HSOC is increased by $26.3 million, bringing its fiscal year 2006 funded level to $61.1 million. This includes an increase of $13.4 million for the Homeland Security Information Network (HSIN) and an increase of $12.9 million to enhance HSOC systems and operations. The funding will provide the HSOC with critical tools for sharing both classified and unclassified information and situational awareness with Federal, State, local and tribal governments.

Fourth, a key element of the Department's Maritime Security Strategy is to enhance Maritime Domain Awareness (MDA), leveraging technology to improve sharing of accurate information, intelligence, and knowledge of vessels, cargo, crews and passengers, mitigating threats to the security, safety, economy, or environment of the United States. The fiscal year 2006 budget funds several key MDA initiatives, including $29.1 million for the nationwide Automatic Identification System (AIS) and $16.5 million to provide additional maritime patrol aircraft flight hours in support of detection, surveillance and tracking activities.

Finally, the Department is seeking additional technology investments in other critical areas, such as:

—$20 million for developing a Low Volatility Agent Warning. This system will serve as the basis for a warning and identification capability against a set of chemical agents whose vapor pressure is too low to be detected by conventional measures;

—Increasing Counter-Man Portable Air Defense Systems funding by $49 million to a total of $110 million in the Budget. This program will continue to promote the viability of technical countermeasures for commercial aircraft against the threat of shoulder-fired missiles by improving reliability and affordability.

CREATING A 21ST CENTURY DEPARTMENT

The Department has made significant progress in strengthening the management of its business processes from inception to implementation. The Office of the Under Secretary for Management focuses its efforts on the oversight, integration and optimization of the Department's human capital, information technology, financial management, procurement and administrative operations. Over the past year, this office has made strides in designing, planning, and supporting new standards for business processes and resource allocation in order to achieve a cohesive organization while ensuring maximum return on investment. This organization is focused on establishing the overall framework, developing management methods, and monitoring the progress of each management function.

Examples of major enterprise initiatives included in the Budget that contribute to Creating A 21st Century Department include the following:

—The program for electronically managing enterprise resources for government effectiveness and efficiency—or eMerge2—to continue implementation of a DHS-wide solution that delivers accurate, relevant and timely resource management information to decision makers. The Budget includes $30 million for this program. By delivering access to critical information across all components, the Department will be able to better support its many front-line activities. It focuses on the areas of accounting and reporting, acquisition and grants management, cost and revenue performance management, asset management and budget that will be integrated with MAX HR.

—MAX HR funding of $53 million involves designing and deploying a new human resources system. The $53 million is requested to support the development and deployment of the new HR personnel system as published in the Federal Register on February 1, 2005. These funds will be used to fund the detailed system design for our labor relations and pay-for-performance programs, provide appropriate training and communication for our managers and employees and to provide proper program evaluation and oversight. In this effort, our goal is to create a 21st Century personnel system that is flexible and contemporary while preserving basic civil service principles and the merit system.

—The Information Sharing and Collaboration (ISC) program will affect the policy, procedures, technical, business processes, cultural, and organizational aspects of information sharing and collaboration, including coordinating ISC policy with other Federal agencies, drafting technical and operational needs statements, performing policy assessments, and analyzing new requirements. The total funding for fiscal year 2006 will be $16.482 million.

These initiatives will help move the Department toward an efficient and effective shared services environment, avoiding duplication of effort across the program areas.

CONCLUSION

Two years ago, Congress and the President took on the enormous undertaking of creating a new Department whose central mission would be to secure the homeland. Under Secretary Ridge's leadership, the entities that now comprise the Department of Homeland Security unified under this overarching goal. As I have become acquainted with the many talented people of the Department, I am impressed by all that they have accomplished thus far. But there is no time to pat ourselves on the back.

As the Department initiates our second stage review, organizes around missions, eliminates duplications, and adopts a risk-based approach, we must identify our crosscutting functions and ensure that we are thinking innovatively how to best exploit our intelligence capabilities, develop policy functions, execute our operational tasks, and implement our long-range preparedness planning.

I thank the Congress for its support, which has been critical in bringing us to this point. I am grateful to be here today to talk about the work we are doing to make America a safer home for us, for our children and generations to come. Thank you for inviting me to appear before you today. I look forward to answering your questions.

NUMBER OF BORDER PATROL AGENTS NEEDED

Senator GREGG. It is hard to know exactly where to begin, because there are a lot of issues here. But let me begin with some of the higher priority items as I see them. And I congratulate you on the risk management approach. I think threat is the issue to finding threat and then responding to it.

Clearly, one of the priority issues from the standpoint of threat is who is coming into the country and where they are when they get here, and who they are when they come across. There have been a whole lot of amendments floated this week on expanding the number of border patrol agents. I actually asked the folks down at border patrol if they had an assessment as to how many agents they needed and where they needed them, and I was told that, no, they did not.

I found that to be a startling fact, in the sense that I would have presumed that there has been a study done within the last 2 years as to where the agents are needed and to what numbers are needed. Obviously, there has been a significant movement of agents to the northern border.

I guess my question is: How many border patrol agents do we need and where do we need them——

Secretary CHERTOFF. Well, again——

Senator GREGG [continuing]. In comparison to where we are today? Congress has, as you know, required an increase of agents by 2,000 each year for a 5-year period.

Secretary CHERTOFF. I know that in the Intelligence Reform Act authorizations were put in place for 2,000, going forward. The President's 2006 budget looks for an increase of slightly more than 200.

I can tell you, because I have sat with Border Patrol, that we do have a comprehensive picture of where we need to deploy our resources. We had an Arizona Border Control Initiative last year, which was successful. This year, I guess about a month ago, we rolled out a follow-up to that initiative, and in talking with Commissioner Bonner and the other leaders of the Border Patrol about

how to do that, they took a very unified approach to figuring out where the sectors of the border where we are now seeing the greatest penetration.

How do we deploy not only Border Patrol at the front line, but technology, and also a capability to transport people that we apprehend and bring them back in a way that does not pull people off the line in order to drive them several hours back to Tucson.

How do we use checkpoints? How do we use investigative resources to target organizations? And also, frankly, how do we work with the Mexicans on their side of the border to see that they are doing things to attack these human trafficking organizations.

So I do think that we have a comprehensive plan about dealing with the issue of deploying resources in a unified——

TRAINING OF BORDER PATROL AGENTS

Senator GREGG. But is 2,000 the right number, a year? And can you train—how many people can you train—let us say we actually funded 2,000, which clearly we are not going to do, but we are going to significantly increase the funding. In fact, Senator Byrd has a proposal to do that, which I presume he is going to offer within the next day or so, and increase border patrol agents.

STATUS OF TECHNOLOGY IN USE ON THE BORDERS AND DETENTION SPACE

How many agents can you train? And two, what's the status of the unmanned vehicle program and did it work? And if it did work, why is the line basically being shut down? And three, what's the status of the electronic surveillance in the cameras? And four, how many detention beds do we need? We hear about a lot of people being sent home who are criminals and who should probably be detained permanently here to make sure they do not come back to commit further criminal acts? How short are we on the detention bed area?

Secretary CHERTOFF. I might forget all this, so if I do, I mean to come back. I'll give you the answer. With respect to training, obviously, the President's budget talks about 210. We can certainly train and assimilate that. I do not know that this is the limiting number in training, but I would also be inclined to agree, I doubt we could train 2,000 even if one had 2,000.

Certainly, we can train and deploy the 210 that we have asked for on top of whatever we are replacing in terms of attrition.

The UAV program, as I understand, did work well. We are currently working now to begin the process of procuring UAVs. We would like to get that done in a matter of months and start to put UAVs up and have them flying over the border.

Now I don't think we can rely exclusively on UAVs. I think that sometimes you need manned vehicles and you need helicopters. But I think it was generally viewed as a positive program, and we are in the process of getting the RFIs and RFPs out in order to make sure that that gets done.

As far as detention beds are concerned, again, the budget contemplates adding some additional beds. I do want, I guess, to address an issue which seems to come up a lot when we talk about releasing people. The fact of the matter is, we do not detain every

single illegal person that we apprehend. And frankly, I have to say, as a graduate of the criminal justice system, neither does the criminal justice system.

Most people who are arrested in States all over the country get released on bond. What everybody does, whether they are criminal justice people or people in the immigration areas, is prioritize. And I do think we are working very hard to make sure that the people who are mandatory detainees are being detained and that we have adequate beds to do that.

ELECTRONIC SURVEILLANCE

Senator GREGG. And the camera situation that allows electronic surveillance on the borders?

Secretary CHERTOFF. I beg your pardon?

Senator GREGG. The camera situation relative to electronic surveillance. I mean there was a contract let that appears did not work and now I guess they are trying again. What is the status on it?

Secretary CHERTOFF. I gather, and I think this is under investigation, there was a contract let and there were some problems with the procurement process. This goes back a number of years. The procurement phase of that contract is over. Obviously, we are maintaining.

My understanding is that as a general rule the surveillance stuff does work well. Obviously, we have maintenance issues. We are now going to begin the second stage of that, which is the America Shield Initiative, where we are sending out RFIs and RFPs to begin the process of acquiring technology.

Obviously, we are going to learn something from the procurement problems in the last round that go back several years, but again, it is a very good technology. I mean the idea of using cameras and remote sensors does work. As long as we get, you know, the right contractor and the right equipment, and it is handled in a cost-effective manner, I think that is a very promising way to go about handling it.

Senator GREGG. Well, maybe you could have your staff tell us whether or not—we know we had the wrong contract. We spent a lot of money.

Secretary CHERTOFF. Right.

Senator GREGG. We bought cameras that did not work. Supposedly, this has been corrected. We would like to get some specifics on that.

Secretary CHERTOFF. We will get back to you on it.

[The information follows:]

BACKGROUND ON GSA BASIC PURCHASING AGREEMENT WITH IMC

The Remote Video Surveillance project was formed in 1998 to install camera systems mounted on poles or towers near the U.S. Border. These cameras would transmit video images back to a control room where a Law Enforcement Control Agent (LECA) could view the images and dispatch Border Patrol agents as necessary.

The Immigration and Naturalization Service's Office of Information Resource Management (OIRM) managed the RVS program. From its beginning, the OIRM faced tremendous pressure to get RVS poles installed or face losing their funding. At first, the OIRM administered the RVS Project through a series of individual purchase orders with various contractors. OIRM would give bills of material (BOMB) to NTMI, a GSA FAST contractor, for the equipment needed for the installations.

NTMI would procure the equipment and store it until needed for an installation. Chugash was the contractor used to install the poles, cameras and monitors. IMC was the contractor used to install the microwave transmission equipment.

A competition was conducted in 1999 in order to increase accountability for the installations and to obtain volume discounts for the equipment involved. GSA considered four companies for this award: the three listed above and Hazmed, a contractor that has assisted OIRM in managing the purchase orders for the other three contractors and that had core competencies in the area of installing electronics systems. IMC was selected as the contractor in March 1999 and given an initial task valued at $2 Million.

In November of 2000, in an effort to optimize procurement procedures, OIRM and GSA agreed to convert the GSA schedule award to a Blanket Purchasing Agreement (BPA). The rationale for the BPA was that it would "further decrease costs, reduce paperwork, and save time by eliminating the need for repetitive individual purchases from the Schedule contract."[1] The end result was to "create a purchasing mechanism for the Government that works better and costs less."[2] The hope was that the reduction of costs would allow for funds to accelerate deployment of additional RVS systems.

Installation of RVS sites was completed in three phases. The first phase involved administrative preparation (i.e., environmental assessments, rights of entry (ROE), real estate issues, permits, and survey activities). Phase I activities generally required between 16 and 18 months to complete. However, there were often issues with access to the land desired for the surveillance site, or environmental assessments, which caused greater delays.

The second phase of the installation involved groundbreaking activities such as installing foundations and poles, assembling and populating platforms, installing power, aligning equipment and radios, and installing equipment shelters. This phase took between 3 and 6 months.

The third and final phase lasted approximately 1 month. It involved installation of the cameras, transmission lines, consoles, other related electronics and the build out of control rooms. Finally, after completing build out of the control room and successful integration testing, the Border Patrol agents would begin using the RVS system. The timeframe for an average RVS installation varied between 20 and 25 months. $239 Million was allocated to GSA for the RVS BPA. Approximately $220 Million was expended by the contractor during its term, which ended on September 30, 2004. At that time there were 248 completed RVS sites. Since that time, six more sites have become operational for a total of 254 sites. The Border Patrol is working with GSA and the contractor to finalize the credits due back to the government for incomplete installations.

Currently the Headquarters Office of Border Patrol's Integrated Project Team is seeking contractor support to complete the installation of 21 Phase III RVS sites partially installed by L–3 Communications Corporation. Government furnished equipment bought under the terms of the BPA will be used to complete the 21 sites. The Headquarters Office of Border Patrol projects these 21 sites will be completed by the end of calendar year 2005.

Senator GREGG. I think I have certainly used up my time, although this clock does not seem to be working correctly.

But in any event, Senator Byrd, did you want to make an opening statement or pursue questions? It is—obviously, the floor is yours.

STATEMENT OF SENATOR ROBERT C. BYRD

Senator BYRD. Thank you. Thank you, Mr. Chairman.

And thank you, Mr. Secretary. Mr. Secretary, you and the 179,000 employees in your Department are to be commended for your efforts to preserve our freedoms and secure our homeland. I applaud Chairman Judd Gregg for taking on the challenge of chairing this subcommittee.

---

[1] The Immigration and Naturalization Service Integrated Surveillance Intelligence System (ISIS) Equipment and Services Blanket Purchase Agreement (BPA) between GSA Federal Technology Service (FTS/FAST) Region 5 and the International Microwave Corporation Team, GS05KR01BMC0001, dated November 8, 2000, page 2 of 12.

[2] Ibid.

His predecessor, Senator Thad Cochran, did a superlative job as chairman. Under Chairman Cochran, this subcommittee worked on a bipartisan basis to provide the Department of Homeland Security with resources to fill critical gaps in our security. Of course, you should know, and I am sure you do know, Mr. Secretary, that Chairman Gregg brings excellent credentials to this task.

As a former governor, he understands that simply setting a policy in Washington does not automatically make that policy a success. We have to work effectively with State and local governments and with the private sector to protect the homeland.

Years before the tragic events of September 11, Chairman Gregg led the way by funding State and local antiterrorism programs. He authored provisions for training and equipping first responders for chemical and biological attacks.

In fact, if you want to meet the father of the Office of Domestic Preparedness, the predecessor to your office of State and Local Government Coordination and Preparedness, I am sitting right next to him, on my left, today.

Mr. Chairman, I look forward to our partnership on this subcommittee, and I thank you for taking on this assignment.

I thank you, Mr. Secretary, also. As the Secretary of Homeland Security, you are responsible for a critical balancing act. We are a Nation that thrives on liberty, but 9/11 taught us that we also must invest in our security. I hope that you will work with the Congress to make sure as much as possible that your Department promotes our security without sacrificing our liberty.

I wrote to you on March 2 to express my dismay that the President's budget fails to fund the border security investments authorized by the Intelligence Reform and Terrorism Prevention Act of 2004 which he signed into law on December 17 of last year.

That Act authorizes the hiring of 2,000 new border patrol agents per year for 5 years, the hiring of an additional 800 immigration investigators per year for 5 years to enforce our immigration laws, and the funding of 8,000 new detention beds for the holding of illegal aliens.

BUDGET AMENDMENT

I urged you to work with the White House to propose a budget amendment seeking resources to increase security on our borders and to enforce our immigration laws. Despite the statements by Secretary of State Rice and former Homeland Security Deputy Secretary Loy that al Qaeda is a threat on our porous borders, there is virtually nothing in the President's budget to provide these additional resources for border security.

According to Former Deputy DHS Secretary James M. Loy, when testifying before the Senate Select Committee on Intelligence about threats to the United States, "Current intelligence strongly suggest that al Qaeda has considered using the southwest border to infiltrate the United States." According to Secretary of State Condoleezza Rice, "we are all concerned about terrorists and how they might use our very long and porous borders. The terrorists are going to keep trying. They're going to keep trying on our southern border. They're going to keep trying on our northern border."

So, I could not help but be disappointed to read your response to my letter yesterday that no budget amendment would be forthcoming.

The threat to our security is clear. The holes in our borders are well known. I look forward to hearing from you on this and other issues today. I thank you, and I thank you, Mr. Chairman. I thank all the Senators.

Senator GREGG. Thank you, Senator Byrd, and thank you for your generous comments. Did you wish to proceed with questions at this time?

Senator BYRD. Would you please have someone else go and then call on me at your leisure.

Senator GREGG. All right.

Well, then I think I would turn to Senator Feinstein, I believe, was the first member of your party here.

Senator BYRD. Very Well.

STATEMENT OF SENATOR DIANNE FEINSTEIN

Senator FEINSTEIN. Thank you very much, Mr. Chairman.

I want to say, Judge Chertoff, that at least for this Senator you are so far a breath of fresh air, and I am delighted to say that. I just want to publicly thank you for your response of April 6 in the use of fraudulent passports, stolen or lost passports, which is a big problem.

I know that from the intelligence committee. And your letter was no-nonsense, and it set forward very directly what the Department is prepared to do. I, for one, will certainly hold you to it.

And I am very pleased that you share my concerns about the visa waiver program, and indicated, you know, that you share the findings of the critical reports that have been done, and that you have established a visa waiver program oversight unit. So I look forward to—my understanding is that you are probably going to come in asking for another extension on the visa waiver program.

My vote, as you know, is conditioned on getting the management act together in that unit, which critical reports have said has been in disrepair for some time. So I just wanted to say that.

BORDER PATROL

I want to follow up on what the chairman said on the border patrol. The expansion of the border patrol is not really just the recommendation of the 9/11 committee. Those of us on the judiciary committee have recommended this for a long, long time, and specifically, the border reform and visa entry law recommended an enhanced border.

As you know, 600 agents have retired this past year. So on a four-to-one basis, whether the 210 additional agents is actually going to provide you with a net gain or not, I think, is somewhat dubious, and I am really concerned about it. The position of the border patrol on 2,000 agents, going back 6 years, has always been they do not need them, they do not have the room to train them. I mean this goes on year after year after year. The time has come to fish or cut bait. That is no longer, I think, a justifiable response.

Bills have called for this. The President says he calls for it. Although, only 210 will not do it. I would like to get your real answer

to this, because on the southwest border, other than Mexican intrusions have gone from 22,000 in 2002 to 88,000 in 2004. This clearly indicates that the southwest border is being utilized as a point of major penetration into this country by other than Mexicans. If you look at the list of apprehensions made from countries that are terrorist States, there are numbers there as well.

So I have a hard time, in view of the Minutemen coming on the Arizona border, the remonstratives made by this Congress over and over and over again as to why there cannot be a net large increase in border control. This is something I think we are willing to pay for. This is something that I think we would be willing to add. And yet, year after year it is the same kind of 200, which does not make even for retirements. Could you respond, please?

VISA WAIVER

Secretary CHERTOFF. Well, first let me begin by just, if I can, for a moment go back to your visa waiver point. I mean as I think you indicated, Senator, I share your concern. We have to look at the border as a whole and make sure we are addressing every possible point of entry. And I certainly intend to hold the Department to what I have indicated to in the letter we need to do to make sure——

Senator FEINSTEIN. Thank you.

Secretary CHERTOFF [continuing]. Our end is up. And I have spoken to our foreign partners and talked about the importance and I have spoken personally to them about the importance of making sure they have their house in order in terms of tracking and getting us information on this, and ultimately moving to a biometric passport that is resistant to the kind of alteration or counterfeiting, which is obviously a vulnerability.

SOUTHWEST BORDER CONTROL

The southwest border, obviously, is a concern as well. As I understand it, what we are proposing to do in the budget is a net increase of 210 border patrol agents, which would fill those that are leaving and fund an additional 210.

Senator FEINSTEIN. So if I may, that means 810 new border agents?

Secretary CHERTOFF. I do not——

Senator FEINSTEIN. Six hundred have retired.

Secretary CHERTOFF. I think new. As I understand it, new means over and above what we currently have, the funding level we have. So that we will wind up at the end of the day with—and I cannot do the math in my head, but I guess there is approximately 10,800 currently. We would be adding about 200. That should include backfilling for positions that are becoming vacant. I mean that is keeping the funding level steady and then adding 210.

So that is what we contemplate, in addition to which we want to be able to bear the UAVs. As I told Chairman Gregg, we want to acquire those and start to put those up. I think that was a successful pilot program, no pun intended. And we do want to do more with sensors, which, again, notwithstanding the contracting issues, apparently, several years ago, we think the idea of the sensors and the usefulness of sensors is proven. So we have an America Shield

initiative and we are in the process of setting out RFIs in order to start acquiring that technology and deploying it.

This is obviously an issue that we have to constantly look at. I am going to go down to the border at some point in the next month or two. I want to see for myself how we are doing down there, and what additional things we can do. We have redeployed agents down to the Arizona border to deal with the issue of a surge of people coming across.

I totally agree with the principle that this is a paramount responsibility of ours, and I am going to be spending a lot of personal time focused on it.

Senator FEINSTEIN. Thank you. My time is up. Thank you.

Senator GREGG. Senator Craig.

STATEMENT OF SENATOR LARRY CRAIG

Senator CRAIG. Mr. Secretary, like all of us, let me welcome you to the committee, and let me also speak, as others have, about our belief that you are the person who can get the job done.

At the same time, let me not sound like a broken record, but let me repeat what has been said here by both our chairman, our ranking member, and certainly the Senator from California. I am going to focus on our southwestern border again.

Because I have been a bit outspoken about immigration policy and changes in it, and I actually led the Senate in debate for the last 2 days on it, I have also been given a lot of attention by those who might criticize any form of policy change, but most importantly, it has led to a lot of conversations about border. And it has allowed me to focus more intently on border. Because I will tell you, if we cannot control our border, we will never be able to write immigration policy that works. We will always be playing catch-up to an ever increasing number of illegals in our country.

The Senator from California and I have discussed this at length. Probably every one on this committee today has a slightly different opinion about how we handle the problem, but I think we are all in concert about how we handle the border.

So my folks in Idaho say build a fence high and build it strong, and spare no cost. Now there are a variety of ways to build the fence, and you're exploring all of them, but there are also not just the physicalnesses of it and all of the tools that we are going to acquire and should acquire to control that border.

There are other issues as to who is there and how they handle process and movement. We have got this interesting situation. Yuma, Arizona. A lot of folks live on the other side of the border, but work across in Yuma. They harvest lettuce. Your folks were out there a few weeks ago rounding them all up early in the morning to come back across the border, because many of them were undocumented illegals. But by 2 o'clock in the afternoon they were back in the fields harvesting the lettuce.

The crisis of the harvest was over, but the reality was that a great deal of border movement occurred during that day. And in that movement, there could have been someone that meant to do this country harm, not just to pluck lettuce from the fields of Yuma, Arizona. And that is something we have to get under control, both sides of that issue.

So let me give you a dialogue that I had with a young man who sought me out because of my position on this committee last year, a very frustrated member of the intelligence community. He and his group were prevented from apprehending suspects at the border because of strict guidelines and the chain of command, even though it was his group's responsibility to collect the intelligence.

His group had gathered immediate intelligence regarding certain aspects and actions needed to take immediate action. However, because of the chain of command and the hamstringing that resulted, certain intelligence agents, this intelligence officer had to sit and watch while suspects possibly crossed the border.

These were not Hispanics. These, by all appearances, were people of Arabic descent. They were believed to be terrorists. And yet the outcome still today is who is on first and who is second and who is in control. And in that fight, people are crossing our borders at an unprecedented rate.

And while we can talk about the money we have spent, and I did on the floor yesterday, billions of dollars, with a "B," and we apprehended a 1,750,000 or 1.2 million last year, or something like that. Big numbers. It demonstrates one thing when we are apprehending them, that they got across.

And I cannot imagine that when someone is illegal, by definition, and they are apprehended, that they are turned loose. At least take them to the border and shove them across. Do not say, "Well, they will come back." They do not come back.

All of us are going to be able to control this process, and I am going to keep pushing for changes in the law that are realistic and that work. But all of a sudden the Senator from California and I are engaged in conversation, and I say my proposal will affect 500,000 or 600,000 or 700,000, and she says, "No, it will not. It is millions."

I do not know whether she is right or I am right. We may both be right in some ways. But we do know there is a huge problem. Enough said.

I guess my question is: Go to the border. Look it over. Get to understand it. It is unique in a variety of ways. And lastly, I was in Houston, Texas, over the weekend. I was visiting with a former State judge, who said to me very directly, there is a clear understanding in Texas that the laws are not going to be enforced because they are unenforceable. And I am talking about border laws.

BORDER PROBLEMS

Now if that is the name of the game along the border, we have got a huge problem that you must get your hands around and get it under control. I agree with the Senator from West Virginia. I am a co-sponsor of his amendment to pull money in this emergency supplemental to give you more. Either build the fence or we do something that causes that border crossing to stop. How do we do it?

Secretary CHERTOFF. Well, first of all, Senator, there are a number of things you raise, and I hope I keep them in mind so I can address them all. I think it is important, as you say, to look at this as a comprehensive issue, not an issue you can deal with in terms of individual slices of policy.

TEMPORARY WORKER PROGRAM

Clearly, one piece of this is the issue of what the President has advocated addressing through a temporary worker program, finding a way to bring some portion of the people who come across the border not to do us harm, but to work, to bring them within the system.

Senator CRAIG. Very important.

STEPPED UP ENFORCEMENT ALONG THE BORDER

Secretary CHERTOFF [continuing]. So that we have some control over them, and also we then reduce the pressure and we reduce the demand which gives the trafficking organizations the kind of resources they need to bring bad people across the border. Now that is one piece of a comprehensive package. Another piece has to be stepped up, enforcement along the border, including better deployment and more efficient deployment of border patrol, use of technology to give us a better span of control over who is coming across the border.

Absolutely, the idea that there are laws that are tacitly not going to be enforced is dead wrong, and something certainly I do not endorse.

When you talk about chain of command issues interfering with somebody apprehending persons coming across illegally, I have to say, I mean if there are bureaucratic obstacles to enforce in the law, I want to get rid of those. I have spoken to Border Patrol and to Commissioner Bonner about, in fact, breaking down the stove pipes that I think used to be. We used to have very regionally controlled, border sector controlled deployment of resources so that you had seams between the regions. Everybody took the view that, hey, I am going to worry about my region and that is all I am going to worry about.

We have now moved away from that. Commissioner Bonner has put together a much more nimble program for deploying resources, which I think, again, is trying to break down those stove pipes. When I hear about these kinds of bureaucratic things, I do want to go out and see what the problem is and try to fix it.

This problem has been around for a long time. When I was U.S. attorney back in the early Nineties we were talking about this. So I know it is not a new problem. I know there is a new urgency. And I think although there is a lot to discuss in terms of detail, I think there is a general view we have to take a comprehensive approach. And I really look forward to working with you and with everybody who is interested in this in putting together a comprehensive policy.

Senator CRAIG. Thank you.

Senator GREGG. Thank you. Senator Murray.

STATEMENT OF SENATOR PATTY MURRAY

Senator MURRAY. Well, thank you very much, Mr. Chairman.

And, Mr. Secretary, thank you for being here today. You have been handed a very, very difficult job, and I commend Senator Gregg for his opening statement and agree we need an honest as-

sessment from you of what resources we need for all of these difficult challenges.

PORT SECURITY

I think everybody here shares the same goal of doing everything we can to make sure our country is secure and it is always difficult when we feel like we are not getting what we really need. We have heard a lot about border security. I obviously am concerned about the northern border. I know all 200 of those, plus, are going to the southern border. We know that the northern border is a problem, but let me set that aside, because I want to focus on port security and cargo security, which you and I have had some time to talk about.

I am very concerned. The Coast Guard commandant testified before us that it would take more than $7 billion to implement the Maritime Transportation Security Act. So far, Congress has provided a little over $500 million of that. I do not think any of that was requested by the Administration. That was Congress adding those dollars in.

Now for the past 2 years, about a billion dollars in port security grants have come in to your agency, and the American Association of Ports Authorities say they need at least $400 million to help secure port facilities this year.

From our discussions I know port security is an important issue for you. You understand it is not only human life. It is economic disaster if we do not secure our ports. But it is disconcerting to me that the Administration does not ask for the dollars for these port security grants.

Does the Agency just discount all the intelligence reports that tell us our ports are a significant risk, or what can we expect on this?

Secretary CHERTOFF. No. I mean I do think ports are a very significant part of the infrastructure we have to work to protect. One thing I want to emphasize: You know, as we go through this process of reviewing the entire operation of the Department over the next couple of months, I try to look at the issue, whether it be ports or rail or aviation, in terms of an outcome or an approach.

In other words, I don't want to know what each agency is doing. I want to know what we are doing in combination to deal with the issue of ports or rail or aviation, because that gives us our total sense of how good we are doing or how well we are doing in protecting ourselves.

There are a number of dimensions to this. First of all, there is container security. We have begun a container security initiative, which pushes our screening and inspection process overseas. That is a very positive——

Senator MURRAY. Well, I want to ask you about that separately in just a minute. What I want to ask you about first of all, is the port security—under the Maritime Transportation Security Act, our ports have to harden the ports, and they are just not getting the resources to do that.

Secretary CHERTOFF. We want to make sure they get adequate resources, bearing in mind, again, with the philosophy of risk management, that we have to prioritize.

Senator MURRAY. But the Administration is not requesting any money to do that, despite the fact that the commandant of the Coast Guard told us we needed $7 billion to do that.

Secretary CHERTOFF. Well, I do think we have money in various grant programs that are requested in the budget that are available to be used for purposes of strengthening ports. We have infrastructure, proposing an infrastructure protection program. We have State grants. We have urban assisted—UASI grants.

We have a lot of different kinds of types of grants, but I also have to say I think that the issue of how we protect the ports has to be looked at comprehensively. Coast Guard plays a role in that. Private parties play a role in that, and have——

Senator MURRAY. I understand that——

Secretary CHERTOFF [continuing]. Private obligations.

Senator MURRAY [continuing]. But under the Maritime Security Act we directed all of these ports to give us a plan of how they were going to protect their ports, which they did. And they now have to implement it. They are not getting any money to do it. And we need a direct targeted program, the Port Security Grant program, to do that.

So I want to work with you on that. I am just disappointed every time when the budget comes over with no money for that, because as you and I both know, a disaster at one of our ports is going to dramatically hurt not only human life, but the economy of this country, whether you are in a port city or not.

CARGO SECURITY

But the other part of that is cargo security. And as you know, I have been really pushing to get some kind of coordinated port security regime in place. Everyone out there is trying their best to move those ports out, to follow our cargo from where they are loaded, into our ports here, and there is no coordinated approach to that.

In the committee report from last year, we directed the Undersecretary of Border and Transportation Security to help us develop a plan for that coordinated approach. It was due February 8. We still have not gotten that yet. And I just feel like—we need the Administration—I have talked with you about this. I have talked with Commissioner Bonner. I have talked with a number of folks about it. And all we get is, "We're going to study this." I know that you and I agree this is an important issue.

How can we help you come up with a coordinated approach to secure our ports, all the cargo that moves through them, and the people who work and live there?

Secretary CHERTOFF. Of course, I am very sensitive to being—you know, not saying we are studying something. So let me be a little bit more concrete.

Senator MURRAY. Thank you.

Secretary CHERTOFF. We need to take the issue of cargo and container security to whatever is considered to be the next level of systems sophistication. There are people in the private world who are very, very good at tracking everything, from point of departure to point of arrival. And there are processes and technologies that

allow us to do that. And that is the kind of system we ought to be looking to moving toward in our container security initiative.

CSI is part way towards that. The principle of moving this overseas is a good step in that direction. We have been meeting with, for example, the private sector, and shipping companies, to talk about ways we might, with greater specificity, track cargo from the time that it departs the manufacturer to the time it gets to the point of arrival, working with the private sector to have them build a security envelope.

And again, through the C–TPAT program, we have got that process as a precedent. We do use that kind of process, so that eventually what we can do is put as much of the cargo through a security envelope from point of departure to point of arrival as possible, track it, screen it, have private sector take a lot of responsibility within that envelope for maintaining security, use technology to make sure we are not getting penetrations, and then, again, you are always going to have some cargo that does not fit within that envelope.

We are deploying technologies like VACAS radiation portal and our National Targeting Center to focus on that subset of cargo that really needs a much tougher regime of screening and inspection. So that, I think, this is the way forward. And I do think we are working with a lot of diligence and a lot of urgency to move into that next level.

PREPARED STATEMENT

Senator MURRAY. Well, I appreciate that. Mr. Chairman, it is a very complex problem. There are a lot of players in it, and what I think is most disconcerting to me is that we do not have a coordinated approach. Mr. Secretary, I hope we can get that report from you that was due February 8 so that we can really start moving forward to get that accomplished.

[The statement follows:]

PREPARED STATEMENT OF SENATOR PATTY MURRAY

Thank you Mr. Chairman. I want to join you, Senator Byrd, and the rest of our colleagues in welcoming Secretary Chertoff to the Committee.

Mr. Secretary, I want to thank you for taking the time to meet with me prior to your confirmation. We had a good discussion about many of the issues we are going to talk about today.

I know that you are still new to the job and understand that this budget request was formulated before you were nominated.

I also understand that you have been handed a tough task in a very difficult time. But from our private conversations, I know that you are committed to keeping our country safe—and I look forward to working with you.

That being said, I fear this Administration—through this budget request—is failing in this most important responsibility.

Mr. Secretary, as you are well aware, the Department you now lead faces enormous challenges.

Concerns that DHS is not meeting the Nation's security challenges are growing—in the Congress, and among the American public.

Don't get me wrong, in fact, I believe Secretary Ridge and Admiral Loy did the best they could with the hand they were dealt.

Merging so many complex entities into one organization was a monumental challenge. We all knew success wouldn't come overnight.

But many of DHS' problems were created by this Administration because it didn't request adequate funding.

Mr. Secretary, the Administration has many priorities—we all do.

The bottom line is that current White House fiscal policy isn't consistent with providing the resources DHS needs to provide the level of security the American people deserve.

To compound this problem, DHS has spent what funding has been available in a scattershot way. There appears to be very little rhyme or reason to how funding is allocated compared with actual threats.

And, we are hearing about it on a daily basis.

Just this morning, we're reading newspaper reports about financial mismanagement at TSA. I don't want to get into that now because I know you'll have an opportunity to respond this morning.

But please know that it just makes it harder for us in Congress to help DHS succeed.

Mr. Secretary, I want to work with you to ensure our budget will actually deliver the security we both seek for our country.

But if we are going to work together, we need to be honest about what resources are necessary to do your job and let the Congress worry about budget priorities.

For example, adding to what I believe is already an insufficient budget request, the Administration assumes user fees that we all recognize are not going to be approved.

In fact—$2 billion of the $2.5 billion increase in the Administration's request would come from a 60 percent increase in airline passenger fees.

Fees placed on the back of an industry that we all know is having significant financial difficulty.

Mr. Secretary, these "proposals"—if not accepted by the Committee—only make the funding problem worse.

As I'm sure you are aware, the Senate has included $276 million for Immigration and Customs Enforcement (ICE) in the Emergency Supplemental Appropriations bill.

This is funding that we all agree your agency desperately needs. In fact, many of us have known about this issue for quite some time.

Last year, I asked Commissioner Bonner and ICE Assistant Secretary Garcia about a news report highlighting a budget shortfall that would result in a hiring freeze at ICE.

At that time, I was told the problem was an accounting error resulting from combining budgets from legacy agencies.

Now it's clear that it was a real budget shortfall and the Senate was forced to include this as new money—designated as an emergency—to enable ICE to lift its hiring freeze.

Curiously, this money was not part of the Administration's supplemental funding request.

Mr. Secretary, the Senate's action speaks volumes about how much we want this agency to succeed, but we need the Administration's help.

We need realistic annual budget proposals—not reprogramming requests and not emergency supplemental requests.

Mr. Chairman, I don't say this to denigrate the performance of any of the hard working men and women who serve us so ably on the front line. Like Secretary Chertoff's predecessor, they are doing a tremendous job with the tools they are provided.

But, this Committee—and the Congress—must do a better job of providing oversight to this agency because right now we are failing the American public.

Mr. Secretary, I know that you, Chairman Gregg, Senator Byrd and the rest of our colleagues care about these issues as much as I do.

And, I don't want to dwell on this too much—but I think it is important context for the other specific issues that I'd like to discuss here today.

I'm quite concerned that good intentions are not going to help us:

—Establish a rigorous port and cargo security regime,

—Protect our borders, or

—Train our personnel correctly

Mr. Secretary, I look forward to your testimony, working with you to address these issues, and ensuring our budget will actually deliver the security we both seek for our country.

Thank you Mr. Chairman.

Senator GREGG. Thank you, Senator.

Senator Allard.

STATEMENT OF SENATOR WAYNE ALLARD

Senator ALLARD. Thank you, Mr. Chairman.

And I also would like to join my colleagues and welcome Secretary Chertoff here this morning. I am also new to the committee here, Mr. Secretary, and I am looking forward to serving under the able chairmanship of Senator Gray.

I wonder sometimes if maybe we are not looking too much to a Federal solution and perhaps should not think a little bit more about what the local law enforcement along the borders. That is the counties along the borders. It is the States along the borders.

This is homeland security. Everybody is talking about more money for Customs and more agents and whatnot, but I happen to believe that those people down along the border that form the Minutemen organization have some real concerns. I think they are really concerned about their property. I think they are really concerned about the safety of their families.

I do not know whether any thought has been in trying to do more to support our local law enforcement along the borders. They are local elected officials. They know about those things. They understand the problems of their community. I wonder if we should not do the same thing with the State. The governor is elected by that State.

I wonder if we should not consider targeting those counties, share with them more of the technology that we have developed at the Federal level, and take citizen groups, incorporate them. Deputize them. Have the local sheriff deputize them or whatever, or have your National Guard or whatever, bringing some responsibility.

I am not implying that they have not been responsible at this particular point in time, but at least bring them under some organized law enforcement thing that traditionally has relied on citizens. That is why we have deputization process. That is why we have the National Guard.

I wonder how much thought you have given to that, because all I am hearing from this committee and all I am hearing so far in this discussion is a Federal solution. I think we will get a better bang for the buck. I mean they are worth a lower salary level. They have more of a commitment in that safety because they live there. I wonder if you would comment on that.

Secretary CHERTOFF. Well, we do work, actually, in the Arizona border control initiative, we are working. We have had a great working relationship with State and local law enforcement officials now.

I guess depending on what community you are in, some law enforcement officials want to be involved and engaged in the process of enforcing the laws against illegal immigration. Some do not. I do not think we can make them do it.

Clearly, though, we want to work cooperatively, because they are a force multiplier. And when we get well trained and we share information, and we get well-trained State and local enforcement officials, they are a welcome addition to the process of extending our ability to deal with the issue of illegal migration across the border.

Senator ALLARD. Well, obviously, you have been in conversation with local elected officials. I just think we can do more. And I think I will be a voice on this committee, at least, for pushing you towards more of a local solution than something run out of Washington. I do not think we have all the answers necessarily here in Washington.

VISIT TO ONE OF THE PORTS

The other thing that I would like to say in a positive way is there has been a few million years since we have had a coastline in the State of Colorado. So I made a personal concerted effort to visit one of our ports. I visited the port of Miami. And I will have to tell you, I was pretty impressed.

And this is the very thing that you talked about in your previous testimony, I saw happening there. I saw technology developed at the Sandia Laboratories in New Mexico being used at that port. And I have to tell you that I feel much better about our port security.

And I think sometimes we are looking at a 100 percent solution. I do not think the citizens of this country can afford a 100 percent solution. But I think we have to come up with some reasonable solutions that work. And I think what I saw there at the port, it was efficient, where they could handle a fair amount. I saw a lot of dedication there, and I was really pleased. I just have to tell you that.

AIRPORT SECURITY

I think sometimes what we see happening in our airports, I wonder if maybe we have not gotten off track a little bit and expecting too much on security in airports. I think the most important thing we did and probably the most cost-effective thing is we put a door that was secure between the pilot and the passengers. But I do think that we need to take a hard look at what is happening at our airports to see if we cannot come up with some more commonsense solutions to what I see happening. So I think there are some good things happening there.

RUDENESS OF CUSTOMS EMPLOYEES

On the other hand, I have also seen, as I have walked through Customs, and particularly in the State of Colorado, and I have been appalled at the rudeness of the employees there. I come from a State where I want to welcome people to my State as tourists. And I have been sort of appalled at some of the rudeness that I saw at Customs.

So hopefully we can kind of improve our bedside manner a little bit. Remember that we have visitors coming to our country. We have visitors coming to our States.

Secretary CHERTOFF. And they are not all criminals.

Senator ALLARD. And if that—yes. And they are not all criminals. If the Federal employee does not treat them respectfully and with a welcome attitude, it hurts our tourism in our State. So I just want to call that to your attention.

Thank you, Mr. Chairman.

Senator GREGG. Senator Byrd.

STATUS QUO BUDGET REQUEST

Senator BYRD. In fiscal year 2004, Immigration and Customs Enforcement (ICE) removed a record 150,000 illegal aliens from this country. However, we know that more than 10 million illegal aliens reside in this country. Two and a half million illegal aliens have overstayed their tourist or work visas. There are over 370,000 illegal aliens who have knowingly disobeyed orders to leave the country.

ICE teams, Immigration and Customs Enforcement teams, deported 11,000 of them in 2004, but more than 35,000 others were added to the list. The system is not working, and this budget request does almost nothing to fix it.

I have a border security amendment pending to the Iraq war supplemental, which is currently being debated on the floor of the Senate. My amendment is offset, responds to known security shortfalls on our borders, and responds to the concerns of many Americans, including the self-styled Minutemen who are performing a major community watch effort on the Arizona border.

While there are, indeed, slight increases proposed for next year, the fact remains that both the Border Patrol and Immigration and Customs Enforcement are experiencing significant attrition this year. According to your agencies, 137 Border Patrol agents have left the service since the beginning of the fiscal year. By the end of January, ICE had experienced a net loss of 299 positions.

On average, you are filling 2,000 fewer detention beds a week than the level for which the Congress provided funds. The proposed increases for next year merely backfill the losses you are experiencing this year. In short, this is a status quo budget request.

The crisis we are experiencing today on our borders deserves more than a status quo budget. Why should we be satisfied with a status quo budget, Mr. Secretary?

Secretary CHERTOFF. Well, Senator, first of all, my understanding, again, of what we are proposing to do is that we are going to—when we talk about increases, we are talking about net increases. In other words, we are going to fund over 200 additional Border Patrol Agents, 140 additional ICE investigators, almost 2,000 additional beds over and above the current level.

Obviously, when people leave, we always backfill those positions, so that I think you have to add those numbers together. And we are talking about funding that would get us a net up-kick in all those categories.

In fact, in terms of 2005, we have submitted a reprogramming to get more money to ICE so that even this year we can begin the process of starting to do some hiring to move them to the level they need to be.

There is no question there is a serious issue, this whole issue of managing illegal immigration. What we have to do is use a comprehensive approach. We have to be able to have more people at the border, better technology at the border, all of which we are now pushing forward. Better investigative capability. Better and more available use of detention beds. And we are doing some additional things as well to free up beds.

REPATRIATION PROGRAM WITH MEXICANS

For example, we are working with the Mexicans to begin the internal repatriation program in the next couple of weeks, whereby we transport Mexicans who come in back to interior locations so that they do not simply go back across the border, connect up with the same trafficking organizations, and then come back a couple of days later.

EXPEDITED REMOVAL

We are using other kinds of techniques in terms of expedited removal to try to expedite the process of getting people that we do apprehend, moving them, again, across the border back to Mexico.

ABSCONDERS AND VIOLATORS OF RELEASE ORDERS AND RETURN ORDERS

We are now targeting for the first time enforcement of people who are absconders or who are violating release orders and return orders to make sure we are apprehending them, and we are, again, getting them and sending them back across the border. And we have to also be vigorous in enforcing the laws against people who are removed and then in violation of the law come back across the border again. We have not always succeeded in getting the kinds of sentences we need from judges in keeping those people who are violators, repeat violators in prison.

So we are very concerned about it. We are taking steps to move forward on this. I am going to look at this issue. As I said previously to Senator Feinstein, I am going to go down to the border, I think, within the next 2 months and talk myself personally to the local people and our Border Patrol folks down there to keep moving forward on this issue.

SATISFACTION WITH STATUS QUO BUDGET

Senator BYRD. Well, are you satisfied with the status quo budget?

Secretary CHERTOFF. I am not satisfied with the status quo. We need to move forward. We need to be better about keeping our borders policed. We need to be better about tracking absconders. We need to be better about getting people removed efficiently. And I think as we look at the whole issue comprehensively, there are a lot of things we can do to get a better outcome.

Senator BYRD. Mr. Secretary, you did not answer my question.

Secretary CHERTOFF. Well, I think what I——

Senator BYRD. Are you satisfied with the status quo budget?

Secretary CHERTOFF. I think what I am saying, Senator, is I think our budget is not a status quo budget. I think it looks to net increases, and, therefore, I will tell you, I would not be satisfied with a status quo budget or a status quo situation.

Senator BYRD. Finally, Mr. Chairman, we would look forward to your comprehensive approach. My amendment will provide you with real resources to implement your comprehensive approach.

Thank you, Mr. Chairman.

Senator GREGG. Senator Domenici.

STATEMENT OF SENATOR PETE V. DOMENICI

Senator DOMENICI. Thank you, Mr. Chairman.

Senator Byrd, I will follow up on your questions and give my own observation after first saying thank you for the job you are doing. I look forward to visiting the border with you and some of the facilities that we have in our State, such as the DOE laboratories, to make sure you understand the competence in other departments of the government to help you do your work.

Senator Byrd, I would say I laud your concern about doing more than we are doing, which is an answer to a status quo. We cannot stand the status quo. I do not know about a status quo budget. But we also cannot stand a status quo with reference to our current laws on migration and immigration.

I mean they are adding to the problem, because it is a mix-up and a mumble-jumble of things and agents do not know what they are supposed to do. I mean when we catch illegal aliens on this side and send them home, what are agents supposed to do when they come right back? I mean we did then look at it and say they are not doing their job.

Senator BYRD. I am with you.

Senator DOMENICI. It is embarrassing to see that we do not have a bill yet on the floor of the Senate on immigration. This is not a way to deal with immigration on a supplemental appropriation bill. I think you would agree with me. We need to debate this issue thoroughly, and it makes them do their job better and adds to the propriety of the United States.

Senator BYRD. I have been singing that song for many years now.

Senator DOMENICI. It is time. I am telling you, many of us agree with you, finally.

Senator BYRD. Thank you.

OBSERVATIONS REGARDING THE DEPARTMENT OF HOMELAND SECURITY

Senator DOMENCI. Now having said that, first, let me say to you, people wondered when you got this job what somebody with your background was doing. I was at your side all the way, because I know what you are capable of doing. I want to laud you so far with the job you are doing. I want to give you a couple of my observations.

First of all, you inherited a Department that was put together hurriedly. It is consequently a very hodgepodge Department. The sooner you yourself find out what was done that is not done right, what was done that might even be wrong, you ought to be the one finding out about those problems and fixing them, because they are going to be determined sooner or later. There are many of them up and down the chain of command of your Department, and you know that. I do not know how soon you can fix them, but I urge that you do so.

My second observation is: Since we put the Department together this way, there is a multiplicity of activities that are, even though we thought we are putting them all together, that they are not all together, because there are many other facilities that do work of the type you need.

I really urge that even though you have set up in the statute a function and thus a piece of your Department, that you resist your Department creating a total group of experts in every one of those niches. Because many of those experts already exist in the government, and you ought to use them. You are using them. I think you should just make that a policy.

Somebody said, this distinguished Senator from Colorado, who shames me, he has been to see Miami, and I have not been to the border in 6 months, which is my own State. He has been way over there in the port of Miami. I ought to go see what is happening on my border.

The problem is that in enforcing our laws, there exists terrific capacity in our national laboratories, in our Defense Department, and those who are studying unmanned aerial vehicles. You do not have to begin every program within your Department. Do I make sense?

Secretary CHERTOFF. Yes. Absolutely, Senator. I mean I really do not want to rediscover the wheel, particularly if we have the wheel discovered elsewhere in the Federal Government or the State government, and the private sector. I mean we do not have the time to do everything ourselves.

One of the observations I had when I came into the Department, two observations. One is completely consistent with your advice, that we really need to comprehensively review what we are doing. I give a lot of credit to Governor Ridge, and Admiral Loy and everybody who stood up in the Department, which was an enormous challenge. They did a lot in 2 years. It took the Defense Department decades to get to where it is now. And we do not have that time. So we should be willing to examine where we can adjust and make those adjustments.

With your second point, Senator, a lot of what we bring to the table is a network. Nowadays in business, people talk about networking. We do not have to own or employ everybody in Homeland Security. We do not and we cannot. What we have to do is network with what is out there in our other Federal agencies, State and local partners, and figure out a way to make everybody work together and to coordinate those things.

So even in my brief 2 months at the Department I have been very clear about saying that we ought to pay as much attention, if not more, to that networking function as we do to the actual physical assets that we own and the people that we have in our Department.

IMPACT OF NETWORKING

Senator DOMENICI. Well, my time is running out. I am going to make one last observation. I will put it two in one.

First, it seems to me, without question, that what you are doing out there in terms of networking is already having a big impact. I am not one who continues to carp on the fact that we do not have good homeland security, because I contend that nothing has happened since 9/11. And that is not an accident.

I think we are doing a much better job at making it hard for terrorists than we give ourselves credit for. Now I do not need you to answer that, but if you can, you should. I mean everybody is just saying we are not doing anything, but why are the terrorists doing

nothing? They keep saying they want to get America. They have not done anything yet. Thank God. Maybe tomorrow they will do it, and Domenici will be crazy. But that is one observation.

And the second one is that it seems to be obvious that even though we want to address risks, we nonetheless want money to go to the States. And the new bill will do what you suggest, and put more money in risks and less in pork projects, allegedly. But I submit that this does not mean that all the heavily populated States are the harbors of all the risks.

I mean in my State you have two national laboratories filled with nuclear activity, the center of nuclear weaponry. That is all I will say. You know what that means. Now you cannot expect New Mexico with .005 tenths of a percent of the money to assume the risk of the extraordinary activities.

I would hope that if we give you a law that does what I have just said, that you have somebody looking at West Virginia and New Hampshire and New Mexico to say what else is there that is essential to our country and dangerous. I do not mean a football field. That is what people are saying. Every gym and football field, because people will assemble, ought to be protected. I do not know about that. You decide that.

But I do know the place where nuclear weapons of the United States are in abundance shall not say, "Well, that's old New Mexico. It's a rural State." Do you understand what I am saying?

Secretary CHERTOFF. I absolutely do. As you have said, I think risk management is not about size of State or population or things of that. It is about individual pieces of infrastructure, individual networks of transportation. I mean population clearly is an element to be considered, but we have to have a much more sophisticated approach. And I think that is exactly what we want to drive to, is our risk management philosophy.

Senator DOMENICI. Thank you, Mr. Chairman.

Senator GREGG. Thank you. Senator Kohl, I appreciate your patience. Please take as much time as you think you need.

STATEMENT OF SENATOR HERB KOHL

Senator KOHL. Thank you, Senator Gregg and Secretary Chertoff.

I would like to talk about airport screening. For those of us, and it includes I assume most of the people here in this room, we are going through, as you know, a lot more intensive airport screening today than we were prior to 9/11. And yet a report came out this week which indicates that investigators have determined that things like knives, guns, and even fake bombs are still being processed through the screeners without detection.

It is almost incomprehensible. I am trying to figure how that can be after all of the money and the effort that we have put in to trying to improve airport security for travelers. They talk about the need for new technology, additional technology, which we apparently do not have or have not yet been able to spend the money on.

Can you tell us whether or not it is true that airport screening today is about at the level that it was before 9/11, and how soon it is that we are going to be able to improve it.

Secretary CHERTOFF. I read the IG's report and I just spoke with the IG about it, because obviously I was very concerned about that. I do not have an independent way of verifying it, but I am not going to dispute it either.

I was very concerned about the question of how do we move to the next level. Clearly, there are issues involving training and things of that sort, which are important, but I agree with the IG that technology is really ultimately what we have to use in order to get to the next level.

We do have some good pilot projects and we do have some good technology. We are continuing to fund that, and I think that is a very promising development. I have to be completely forthright in saying we also have to make some difficult decisions about policy in order to decide if we are going to capitalize on that technology.

BACKSCATTER TECHNOLOGY

For example, one form of technology that makes it easier to detect these kinds of threats is backscatter technology. That has certain implications for privacy, because it does essentially, in some form, allow you to look to see what someone is carrying on them that they may be concealing. And so there is sometimes resistance to that.

I think we have to be prepared to say that we need to start to deploy these kinds of technologies and make appropriate adjustments for privacy if we are going to get to that next level. The technology is out there and it is being used. It is a question of the decision to deploy it and to try to balance that with legitimate privacy concerns, but not get so caught up in an endless debate about it that in 5 years we are still sitting there with the technology available and useful and helpful, but we have not put it out yet because people are still hand wringing about it.

So I very much want to start to take the step of moving that technology out and continuing to press forward on the research and development side, but also not letting the perfect be the enemy of the good. If we can make things better, let us get them better rather than wait for the magic bullet that is going to solve everything.

IMPROVING AIRPORT SECURITY

Senator KOHL. Yes, it is very surprising to me and I think to every traveler to think that in spite of all the money that we spent and the delays that we now go through at airports that we did not go through prior to 9/11, some people in the position to know are saying that airport security is about at the same point that it was then. This, I am sure, is a matter of great concern to you, and I hope that we can effect some improvements.

Secretary CHERTOFF. Well, I intend to do so. It is troubling. I think we do have good capabilities in technology, and I think we have to now start to move the process forward. And I am very interested in seeing that we do that.

FOREIGN STUDENT VISAS

Senator KOHL. Okay. I would like to talk about foreign student visas for a minute. As you probably know, there has been a signifi-

cant increase in the time that it takes for foreign students to get their visas to enter this country to attend school. And as a result, the number of applications has gone down, the number of foreign students who are enrolling post-graduate has gone down. And universities all across the country are quite concerned about this.

In 2003, it was indicated that 40 leading research universities reported that 621 students missed the start of classes because of visa delays. Now certainly we need to do the job of checking out, keep out those students who should not be here for security reasons, but is there not something we can do to increase our level of ability to move people through the process and allow them to get enrolled in universities?

Secretary CHERTOFF. Well, we should. I have talked to Secretary Rice about this. We have already taken some steps in terms of lengthening the period of time a visa is applicable so that at least once we have passed someone through the screen they have an ability to spend more time without rechanneling themselves through the process. That is a positive development.

Obviously, we need to do more in terms of our ability to vet people in advance, to do it more quickly. And we need to also, frankly, send the message out that we want to be hospitable in doing those things. So I think we are all committed in moving that forward.

Again, I want to be fair and like I said be blunt in saying the schools also have to help, too, because we do encounter situations where people come in for schools and they do not show up or they leave the program. And, of course, we should know about that. The school should report that to us. And certain schools get a reputation as being easy marks for people who want to come and maybe not to study, but to do something else.

If the schools do not cooperate with us, they make it very hard to run the program in a way that helps the entire spectrum of universities. So part of what we need to do is make it more efficient for people to get their visas, give them longer visas, but also make sure the schools live up to their obligation to let us know if people are abusing the system. And that is part of the tradeoff in order to make this work for the best interest of everybody.

Senator KOHL. I thank you very much and I thank you, Mr. Chairman.

Senator GREGG. Thank you, Senator.

Senator Cochran was not able to join us today, but has submitted a statement for the record.

[The statement follows:]

PREPARED STATEMENT OF SENATOR THAD COCHRAN

Mr. Chairman, thank you for accepting the job of chairing this important Subcommittee. You have some big shoes to fill, but I know you can do it.

Mr. Secretary, you are off to a great start. We appreciate your visit to my State and the way you have moved quickly to identify the challenges facing the Department of Homeland Security.

We need strong leadership in this important job and I know you are well-qualified to provide it. The main challenge is to coordinate the Nation's resources in this effort. Our greatest strength is the ingenuity of our public servants and citizens. With the proper leadership, we will meet these challenges.

Our role on this Subcommittee is to provide you and your Department with the resources needed to carry out your responsibilities and we will work with you to identify the priorities.

TSA

Senator GREGG. Let me pick up on your question, because the TSA is an issue that I think just every American is a little frustrated with sometimes. And I guess my question is this, and it is a philosophical one.

Once we hardened the doors and took away the capacity to use airplanes as missiles, private passenger airplanes as missiles, we changed the dynamic of the threat fundamentally. And yet we have created an agency which has what, 45,000 people? And here we are on a border where we have 10,000 agents, and we probably need 20,000 agents to do it right, have to be well trained, obviously, and there has to be an infrastructure to support them, and all that.

Are we basically reacting to yesterday's threat? We have port security issues. We have border crossing issues. And yet we put a huge amount of resources into airport security without, it appears, any significant improvement in security relative to the ability to get weapons through security, and having addressed the fundamental threat, which is an airplane used as a missile.

Secretary CHERTOFF. I asked myself that question coming into this job as well, and if I can just take a minute to break it into several different issues.

AVIATION SECURITY

First of all, there is the issue of aviation security in itself. Are we optimally focused on what the real threat is? And I think you have put your finger on it, Mr. Chairman, when you indicated the first thing we have to be really pretty tough about is recognizing that there are degrees of consequence that we are worried about.

The aircraft as a missile is the worst consequence. It is bad to have an aircraft blown up in midair, too, that may be a somewhat less significant consequence. It would certainly have tremendous ramifications across the airline system, and then there are yet other possible actions. So we have to frame the issue that way.

We do have hardening of cockpit doors. There are other steps we can and should take to prevent the aircraft used as a missile. That might very well counsel to change or moderate or adjust our current levels for screening with respect to certain types of items, and increase our screening for other types of items.

Maybe to use the proverbial example of nail clippers, which I do not think are being screened for now anyway, but maybe we need to be a little less worried about metal cutlery and a little more worried about explosives. So that is within the issue of aviation, and that is something we are actively looking at now.

EMERGING ISSUES

The second issue is making sure our attention is not distracted away from emerging issues. We are looking heavily at the issue of rail security. We are looking at the issue of cargo. We have deployed non-intrusive inspection technologies. Those are very good. I have seen them work myself. You may very well have it as well. That is a positive step we are paying attention to.

And as I said to Senator Murray, we are looking at this whole issue of cargo movement to see how we can use the modern supply

chain, techniques, and technology to really make sure we are doing what we need to do to protect against bad cargo. So I am completely on board with the idea of making sure we are not distracted by the thing we have already done, spending a lot of time on that because we know how to do it and it is comfortable, rather than looking at the stuff we have not done as well that we need to elevate up.

MOVEMENT OF RESOURCES

Senator GREGG. Yes. I agree. And I am glad you are looking at it that way. But I am asking, are we taking it to the next step, which is, you know, we are spending, I think, I have forgotten the numbers, $3.5 billion, some outrageous number, on TSA. But should we be moving that number to border patrol? Should we be taking a large percentage of that employee base and moving them over, if not as a direct personnel shift, as at least a resource shift, reducing the number of personnel at TSA and moving people to border patrol where we know we have a bigger risk right now relative to the potential threat.

Secretary CHERTOFF. Well, I do not know, Senator, that I would do that, because I do not know that I would say that there is a bigger risk. I mean I do not want to go to the other end and minimize the aviation risk too much. I mean the reality is, even putting aside the aircraft as a weapon, if we were to have a series of explosions on airlines, or something comparable, that would have a humongous effect on the national economy and a humongous effect on our ability to move around.

We want to have a smarter deployment of resources in the aviation security area, but we want to have the outcome be very, very good security in terms of things we are worried about. I do not know that, for a whole host of reasons, including training and skill sets, that we could simply move TSA people into——

Senator GREGG. I do not think you could——

Secretary CHERTOFF. Yes.

Senator GREGG [continuing]. Move people, but I am talking about the dollars to support those people. I mean the threat to the aircraft now is, as you mentioned, an explosive probably more than a weapon, because you cannot take control of an aircraft with a weapon, theoretically. I mean maybe it is possible if you have a big enough weapon on board. But if an explosive is the threat, is it not really a technology response to that rather than a people response?

Secretary CHERTOFF. I think that is right. I think ultimately the way to move to the level we need to get is technology, because I think there is an inherent limitation. People are limited by the technology. I mean you can be the best trained and the most well-intentioned person in the world. If your detection device does not let you get sufficient granularity or make distinctions between types of things, between the dangerous and not dangerous, that is limitation. So we need to get the technology to where it needs to do.

That might ultimately allow us to reduce workforce, although I do not want to make a prediction that it is going to happen in the short term, because I still think there is an element of human judgment that you bring to bear that is still very important. But there

is no question that we have to both invest in the technology, but also, as I said, roll out the technology we have and start to use it, rather than continuing to fuss around, you know, everybody having—I do not want to minimize privacy concerns. I have them as well. But we need to come to grips with them, we need to adjust for them, we need to reach a decision about how to accommodate them, and then we need to start to move forward.

THEFTS OF LUGGAGE OF PASSENGERS

Senator GREGG. The problem I see coming here—well, this is just one element of the issue, but relative to TSA—is that with a report of literally thousands of thefts occurring in luggage of travelers, and it appears that a high percentage of those thefts are the responsibility or the actions of Federal employees of TSA, that we are probably going to have to institute a major camera program or something to monitor the search of luggage by employees. And so we are going to end up spending significant resources to protect ourselves from the employees who are supposed to be protecting us from damage on the planes. As a taxpayer I find that uniquely frustrating. And as a policymaker, I find it to be a terrible waste of resources.

Secretary CHERTOFF. I agree. I mean, obviously, pilferage is completely unacceptable. And it is a bad State of affairs if we have to spend money protecting ourselves from people who are protecting us.

I am convinced, of course, the majority of screeners are terrific and ethical and——

Senator GREGG. I am sure that is true.

Secretary CHERTOFF [continuing]. Things like that. But you are right.

Senator GREGG. The track record, unfortunately, is that there is a large amount of—there is a big problem here.

Secretary CHERTOFF. And that is why—I agree with you. The technology is really the way forward in terms of getting ourselves to where we need to go.

DHS INTELLIGENCE ROLE

Senator GREGG. In the area of intelligence, I am not sure I understand, and I am new to this. Since the issue was moved out of CJS, and I am new to this committee, I am not sure I understand what the Department sees as its role in intelligence right now. It is clear that there was a conscious decision to give up the actual collection and analytical effort to other Federal agencies. You got IAIP, which I guess is stood up, but it seems to continually to be raided for its revenues.

What do you see as the intelligence function of Homeland Security, of the Agency, in relationship to these other agencies and internally?

Secretary CHERTOFF. Well, first of all, I think we are definitely in the business of collection. Let me explain what I mean by collection. We have thousands of interactions every day at the border and investigations with ICE agents at the airport. And many of those yield information which I would consider to be of intelligence value.

We are in the process now of increasing our use of that intelligence and our collection of that intelligence, doing a number of different things. For the first time, we are putting reports officers into the operational units, meaning people who will look at the operational flow of information and say, wait a second, this is not just a trivial interaction. This is a piece of information that is useful from an intelligence standpoint. Let us make sure we capture it and send it up to our information analysis section so it can be fused and collected and then ultimately transmitted to the community.

We have started to do that. I have seen the results. The Federal Air Marshals actually use modern technology to in real-time report things they see on airplanes that could have intelligence value in terms of suspicious behavior, so we get identification of people that we need to be on the lookout for and we can then put that into a system that all of law enforcement can have access to. So we have a tremendous potential to be collectors, which I want to make sure we are fully exercising.

The second piece of that is, once we get ourselves to where we need to be in collection and we continue this process, we can contribute to the whole community by putting that into the NCTC, which is the counter-terrorism center. And that was set up by Congress in the Intel Reform bill as the kind of fusion point for counter-terrorism intelligence.

By putting that information in there, we are sharing with the community. We are also contributing. And my experience is that when you contribute as a partner, you then get full partnership. So I view that as a very critical piece of what we need to do to make sure we are sitting at the table with respect to everything else that comes in from the other parts of the intel community—overseas stuff, signals intelligence, human intelligence in other countries.

The third piece is, as partners at the table, we need to be able to look at all that stuff and operationalize it. And right now in the Department we are talking about how we want to enhance the ability of IA, of information analysis, to collect all this from the central pool that we have at the NCTC, to translate into operational mandates to make sure we make adjustments at the border and other adjustments so that we actually make use of this intelligence.

So that is my vision of where we are going. I have met with the acting head of NCTC. I have met with other main players in the community, and I have expressed my very strong personal interest in seeing that we get this done.

USE OF IDENT, IAFIS AND US VISIT

Senator GREGG. Where do you see the technology situation relative to IDENT, IAFIS, and also relevant to US VISIT.

Secretary CHERTOFF. As you know, Senator, IDENT was, I guess, the system that was stood up under the old INS, pre-9/11. IAFIS is a system the FBI set up. Right now, as I understand it, we have the ability at ports of entry, at Customs and border-patrolled posts, to access both of those databases at the same time. They are separate databases, but we can run prints against both of those databases.

Now IAFIS is a ten-print database. So ultimately there is a decision which we need to reach about implementing a way to get to making effective use of a ten-print database. And I think there is a technological challenge there and there are some policy decisions that we are in the process of making.

I think we made a lot of progress in making both databases accessible at a single point at the border and at our border and customs stations. We have not fully exploited the technology. We need to continue the process of building an architecture that lets us get the maximum use out of our biometric data that we capture and run it against the maximum number of databases.

Senator GREGG. US VISIT.

Secretary CHERTOFF. We have deployed it at our airports. We have deployed it at seaports. We have deployed it at our 50 most significant land border entry points. We are starting to pilot it at the exit points.

It has been very successful. I have seen it operate. It is fast. We have captured people on it that we should not be letting in the country and we have been able to turn them away.

You know, it can be improved, and we can make better use of it. But it is, I think, the key to the next generation of keeping our borders secure.

PREPARATION FOR BIOLOGICAL ATTACK

Senator GREGG. What do you see your success relative to preparation for an attack that might be biological?

Secretary CHERTOFF. As you know, Mr. Chairman, we just finished TOPOFF III, which was a massive exercise done internationally and in two States, which had a hypothetical biological attack. I have met with Secretary Levitt. We have talked about some preliminary lessons learned. We are doing a very comprehensive review of that to make sure that we have the following things in place.

First of all, we have an adequate stockpile of the kinds of antidote where we have them or vaccinations where we can have them against the likely agents; that we have very particular plans in place for distributing that type of vaccine or that type of antidote, if we should have an attack; and that we are fully integrated across the board in terms of our standards for reporting biological incidents.

You know, we had that anthrax false scare about a month ago. We did a very vigorous review of that. We have made some changes now with the Defense Department as well as with our Department in making sure we are operating with the same set of standards. And we are now working across the Federal Government to test to make sure everybody has got the same template for what we are sensing, what constitutes a positive finding, when do we get to the point that we need to take steps to get people inoculation or antidote.

Again, we have got progress to make. I think we have learned a lot of lessons, both recently and going back, and I think we have a program in place to start to move ourselves to a position of readiness for what, I agree with you, is one of the two or three worst-case scenarios that we have to be prepared for.

TOPOFF EXERCISE

Senator GREGG. It is interesting. When I was on the Commerce and Justice Committee, when I was chairman of that, we began the TOPOFF exercise program over the strong resistance, ironically, of almost every Federal agency. We simply insisted we do it. It has now turned into a very successful program.

But I was interested when I was at the TOPOFF exercise this year that neither New York City nor Los Angeles were—I guess Washington, marginally, participated in the major TOPOFF exercises there. I guess that is because they have not been asked to do it, or agreed to do it.

It would seem since they are priority areas, that we would want in our TOPOFF exercises to go to places where the actions may actually most likely occur.

Secretary CHERTOFF. I was not involved in, I guess, the selection for 2003 and I guess the selection for the next one was made before I came on. I know people do apply and then a decision is made.

I know Chicago did the last one, I think, TOPOFF II. Northern New Jersey and Connecticut are part of the New York metropolitan area, so we did exercise some pieces of this.

I agree, at the end of the day—by the way, we should be doing tabletop exercises, meaning not maybe the full TOPOFF, but something all across the board. I wondered myself how valuable it was, and I have to say I was convinced that it was of tremendous value.

I learned a lot and I think a lot of people learned a lot by testing the system. So I am in favor of doing at least some kind of exercise as an important part of our preparedness.

Senator GREGG. Well, I would hope that the Department would take a look at whether or not we should not do them to some degree based on the threat criteria versus just the willingness of a governor to participate or a State to participate.

Well, I appreciate your time. I have two last questions.

STABILIZATION OF SENIOR MANAGEMENT

There is a large amount of open slots and acting slots. What do you see relative to senior management getting it up and stable?

Secretary CHERTOFF. I am concerned, obviously, as a secretary who does not want to have to do every job himself, to make sure we have very good people. I am pleased to say we have filled some of those spots. We have got others where we have nominations pending before the Senate. Obviously, the more quickly we can fill those spots the better.

We want to get the right people. We want to get people who have the energy and the creativity to make the Department what I think it can be, going to the next level. And part of what we are trying to do, frankly, is to recruit and bring people in to top slots that bring a variety of different perspectives.

I think it is good to have people with military backgrounds, people with law enforcement backgrounds, people with business backgrounds, people with first responder backgrounds, because ultimately our success involves merging functions, and that means merging skills.

So we are actively out there finding the right people. The President has got some nominations in and has made some appointments already. And I am, for personal as well as professional reasons, very eager to get this process done as quickly as possible.

NEED FOR ADDITIONAL ASSISTANCE FROM THE SUBCOMMITTEE

Senator GREGG. And lastly, beyond approving your budget, which I suspect we will do and actually probably do more than your request, is there anything this committee can do to be helpful in the legislative or other areas?

Secretary CHERTOFF. There may well be as we complete this process of second-stage review that we will have some recommendations to make for some legislative action that would align us better in terms of what we need to be able to generate for outcomes. And I will look forward to when we get to a point that we can, I think, have some recommendations sitting down with you and the other members of the subcommittee and talking about those, and trying to adjust as much as possible.

One thing I do want to thank you for is the subcommittee's commitment to make sure that we get real discretion in terms of using risk management as a way of handling issues like funding and all of our functions, as opposed to—I know from what I read in the paper that the lobbyists continue to view DHS as a wonderful—I think one used in a newspaper article the term "pots of money" for the clients.

I do not view us as pots of money. I view us as having an obligation, both as stewards of the public money and as stewards of the public safety to make sure that what we do with our money that Congress appropriates for us is based on sound judgment and risk management, not based on lobbyists trying to get their clients into the pots of money.

Senator GREGG. Well, I agree with you. In this issue, first off, funds should be distributed on the basis of threat; and, secondly, earmarks should be used only in the extreme situation where Congress has a very legitimate policy reason that feels that the Administration is not pursuing. So I presume that will continue to be this committee's approach.

Secretary CHERTOFF. Right. Thank you very much, Mr. Chairman.

Senator GREGG. Thank you, Mr. Secretary, for all your time. I appreciate your courtesy.

Secretary CHERTOFF. Thank you.

ADDITIONAL COMMITTEE QUESTIONS

Senator GREGG. There may be members who wish to submit questions to the Department. As is typical, we presume they will be answered in a prompt way.

Secretary CHERTOFF. Absolutely.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing:]

QUESTIONS SUBMITTED BY SENATOR JUDD GREGG

COMPREHENSIVE REVIEW OF THE DEPARTMENT

Question. Secretary Chertoff, in your first speech after being confirmed Secretary of Homeland Security; you announced that you had initiated a 60 to 90 day comprehensive review of the organization, operations and policies of the Department as a whole. You discuss that review more fully in the prepared statement which you have submitted to the Committee.

You are now some 30 days into that review. Can you share any of your preliminary findings with us at this point, including any preliminary conclusions you may reach on what's working and what is not?

Answer. The comprehensive review of the Department is complete. I gave a speech on this topic on July 13 where I outlined our preliminary conclusions, the text of which can be found at the following website: http://www.dhs.gov/dhspublic/display?content=4597.

Question. You indicate that the Deputy Secretary Michael Jackson is overseeing this review and has selected a team of Department officials to look at cross-cutting issues and determine how departmental resources and programs can be effectively used to achieve our security goals. Do you intend to involve others outside of the Department in this review?

Answer. Other Federal agencies were included in this effort where appropriate. Moreover, while the committee was comprised exclusively of DHS employees, we considered recommendations from our state, local, tribal, and private sector partners, among others.

Question. What cross-cutting issues are you looking at? How were those determined?

Answer. We looked at all areas to examine the mission and work of all DHS elements to ensure that we have the best organization, operations, and policies possible to most effectively protect and safeguard this Nation. Notable examples of areas in need of greater cross-cutting included maritime cargo security, information sharing, and immigration policy. As a matter of process, the senior leadership of the Department was asked to identify the key issues that should be evaluated as part of the comprehensive review. The issues were then reviewed by me and the Deputy Secretary to identify further and refine cross-cutting topics that encompassed the key issues identified by the senior leadership.

Question. As you are aware, we are fast-approaching the time when the Committee will make decisions on the Department's appropriations for fiscal year 2006. The budget request now before us is based on the Department's current structure and operations. Therefore, we are very interested in staying abreast of what changes are being contemplated and recommended.

What is your time frame for concluding the review and for making any changes you determine are necessary, including those that might be done through your reorganization authority or require the submission of a legislative proposal or fiscal year 2006 budget amendment to the Congress for consideration?

Answer. The comprehensive review of the Department is complete. I gave a speech on this topic on July 13 where I outlined our preliminary conclusions, the text of which can be found at the following website: http://www.dhs.gov/dhspublic/display?content=4597.

We have also outlined our reorganization plan in detail in our Homeland Security Act Section 872 report, which was submitted to Congress after we completed the Second Stage Review (2SR). Further, a few of our recommendations will require congressional action. We have submitted legislation accompanying the 2SR Report that, once passed, will effectuate the reorganization changes we believe are necessary for the Department's success. It is important that our draft legislation be passed in its current form.

INTERNATIONAL PARTNERSHIPS

Question. How will the Security and Prosperity Partnership of North America announced last month promote and foster a mutually beneficial, common security system along our borders?

Answer. On June 27, in Ottawa, Canada, U.S. Department of Homeland Security (DHS) Secretary Michael Chertoff and Department of Commerce Secretary Carlos Gutierrez and their government counterparts in Mexico and Canada released the first report of the Security and Prosperity Partnership (SPP) of North America that identifies initial results, key themes and initiatives, and work plans that further promote the security and prosperity of North America. The SPP countries agreed to these, and other, North American security goals:

—*North American Trusted Traveler Program.*—All three countries have agreed to create a single, integrated program for North American trusted travelers by 2008. Individuals applying for trusted traveler status would be able to apply for the program and pay relevant fees in one transaction. Enrolled participants would have access to all established trusted travel lanes at land crossings, airports and marine programs. A single North American Trusted Traveler Program embodies the intent of the SPP to establish optimum security goals while accelerating legitimate cross-border trade and travel. The United States will also be working cooperatively to identify Western Hemisphere travel document standards required under the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).

—*Preparedness and Incident Management Systems Integration.*—The United States, Canada and Mexico have agreed to transform North American preparedness for response to large-scale incidents by establishing protocols for incident management that impact border operations within 12 months. Protocols will also address maritime incidents, cross-border public health emergencies and cross-border law enforcement response. The SPP countries have also committed to ensure interoperable communications systems and to participate in preparedness exercises that will strenuously test these protocols. In addition, the three countries will participate in a preparedness exercise in anticipation of the 2010 Vancouver/Whistler Winter Olympics.

—*Border Enforcement.*—The United States and Mexico will form joint intelligence-sharing task forces along the U.S.-Mexico border to target criminal gang and trafficking organizations and reduce violence along the border. The United States and Canada will coordinate maritime enforcement programs to address the huge volume of boat traffic in our shared waterways.

—*Facilitated Flow of Legitimate Cargo and Travel Across Land Borders.*—The United States, Canada and Mexico have agreed to review our transportation and border facility needs, in partnership with stakeholders, and develop a plan to prioritize future port-of-entry-related infrastructure investments. All three countries are considering programs to reduce transit times and border congestion by expanding trusted traveler programs to additional ports of entry and partnering with public and private sector stakeholders to establish "low-risk" ports of entry for the exclusive use of those enrolled in our trusted trade and traveler programs. The United States and Canada, along with local stakeholders, are working to reduce the transit times by 25 percent at the Detroit-Windsor gateway within 6 months, and all three countries are exploring ways to expand this innovative 25 Percent Challenge to other North American land border crossings within the next 18 months. By December of this year, the United States and Canada governments expect to complete an agreement on a pre-clearance pilot program at the Peace Bridge in Buffalo, NY, contingent on Canadian legislative amendments. Within 6 months, both countries will also develop a plan to expand the Vancouver NEXUS-Air pilot program to other United States air pre-clearance sites in Canada and examine the feasibility of expanding the eligibility for NEXUS-Air to include Mexican nationals.

—*Shared Watchlists and Integrated Traveler Screening Procedures.*—The United States, Canada and Mexico have agreed to strengthen information sharing related to terrorists and criminals. Effective information exchange among North American countries is essential to strengthening our capability to prevent acts of terror within and outside North America. The United States, Canada and Mexico have also agreed to establish compatible screening standards for land, sea and air travel to identify and prevent high risk travelers and cargo before they depart for North America. Additionally, recommendations will be made on the enhanced use of biometrics in screening travelers destined to North America. On an ongoing basis, the SPP will enable all three countries to address and resolve gaps in cross-border information sharing. Ultimately, all travelers arriving in North America will experience a comparable level of screening.

—*Maritime and Aviation Security.*—The SPP countries will also be working toward comparable standards for hold baggage and passenger screening, implementing no-fly programs throughout North America, and developing new protocols for air cargo inspection. Likewise, we will also be working to develop compatible maritime regulatory regimes and to strengthen information sharing and coordinated operations in the maritime domain.

Question. What role will the Department have in this initiative?

Answer. The Department is taking a lead role in implementing the SPP's Security Agenda, in cooperation with other Federal agencies. The Department has been tasked with convening working groups with Canada and Mexico to develop and implement concrete work plans and specific timetables to meet the broader goals asso-

ciated with the SPP's Security Agenda. Additionally, the Department is continuing to work with the Department of Commerce, which is taking a lead role in the development and negotiation of a complementary Prosperity Agenda, and the State Department, who is taking a coordinating role to best align efforts.

Question. Under the Western Hemisphere Travel Initiative recently proposed, how will the Department ensure that NEXUS is universally available on the Northern Border by the time the new document requirements are imposed at land ports of entry?

Answer. To keep pace with the potential impact of the WHTI, DHS plans to expand the enrollment process as well as potentially opening additional ports of entry with regards to NEXUS program along the Northern Border. Concurrently, we are also examining potential resource needs to accommodate additional demands of these programs as a result of the WHTI. As part of the Western Hemisphere Travel Initiative (WHTI), DHS will be issuing an Advance Notice of Proposed Rulemaking (ANPRM) to solicit comments from the public and affected entities regarding the requirements and alternative documents that may be designated by the Secretary to demonstrate citizenship and identity for entry. As required by the President, we are and will continue to examine, in response to comments on the ANPRM, other potential documents that may be designated for the land border environment in advance of the January 1, 2008, deadline.

Question. How is the Western Hemisphere Travel Initiative going to work with US VISIT, since US VISIT is implementing the tracking of entries and exits across our borders?

Answer. The Department will coordinate the implementation of the Western Hemisphere Travel Initiative with US VISIT enrollment to facilitate travel and to ensure security at our Nation's borders.

Question. Will US VISIT manage this initiative?

Answer. US VISIT is playing an active role in this initiative.

MANAGEMENT AND STAFFING

Question. Executive agencies need to rely on a stable bureaucracy to keep things running during leadership transitions. The Department has significant vacancies in top leadership positions and significant turnover in senior- and mid-level managers.

Mr. Secretary, what is your time frame for putting your management team together?

Answer. I agree that we do not want any unnecessary delays in filling these vacancies. At the same time, however, we want to make sure we get the right people to fill these positions. We want to bring people on board who have the energy, creativity, and a variety of perspectives to further the Department's mission and enable us to move to a next level of achievement. The President has forwarded several nominations to the Senate for consideration, and we will move as quickly as possible to fill remaining vacancies.

Question. What disruptions are the current vacancies in confirmed leadership positions having on the Department?

Answer. For every vacancy in a leadership position, an employee has been identified to serve in an Acting capacity until a person is confirmed to fill the position. While we are striving to fill vacancies as quickly as possible, these dedicated employees have risen to the challenge of fulfilling the requirements and obligations of these leadership positions and have maintained the Department's activities and efforts.

Question. What is your assessment of the difficulties the Department has experienced attracting, hiring or keeping qualified personnel and what is being done to correct this situation?

Answer. DHS faces many of the same problems with recruitment and retention that plague most Federal agencies—cumbersome recruitment and hiring processes, lack of competitive salaries, and poor performance management and recognition programs. Fortunately, our mission is inspiring to many, and we usually are able to attract well-qualified candidates in spite of these impediments. However, we need to continue to improve to stay competitive for the very best candidates.

DHS has a Human Capital Strategic Plan that aggressively addresses effective recruitment, development, compensation, succession management, and leadership issues. A major priority in this Plan has been streamlining the DHS hiring processes to meet the Federal standard of 45 days. A common DHS recruitment brand with state-of-the-art recruitment materials has been established to ensure effective and consistent external representation of DHS in the hiring process. These initiatives will enable DHS to maintain viable recruitment networks, particularly in mission critical occupations.

A consolidated DHS Workforce Plan was completed in March 2005 that establishes a baseline for workforce trend analysis for mission critical occupations. This Plan also enables component organizations to plan well in advance for upcoming recruitment needs. Where potential occupational gaps exist, human capital strategies will be identified and implemented.

MAX, the new human resource system for DHS, will have both market-sensitive pay and a robust performance management process, which will enable DHS to be more competitive in its recruitment process and more effective in retaining and motivating employees.

DEPARTMENTAL REORGANIZATION

Question. Reorganizing seems to be a sport within the Department these days. At what point does continued reorganization impede the ability of the Department to get its job done?

Answer. The Department's reorganization plan will significantly enhance, not impede, our ability to meet our current and future objectives. The Department recently passed its 2 year anniversary mark. In that short time, 22 separate agencies were brought together, and the work of integrating those agencies into a working structure began. We are now taking advantage of 2 years of experience, an opportunity unavailable to our predecessors, to implement a reorganization plan that takes the Department to the next level, best positions us to manage our current and future responsibilities, and helps us better adapt to current and future threats and disasters.

Question. On the other side of this issue is the continued viability of the current organization of the border management agencies. DHS has moved organizations into ICE; it has moved organizations out of ICE. We have poured almost $800 million in additional resources into ICE over the last 2 years, including $276 million in the Senate-reported fiscal year 2005 emergency supplemental. Is ICE a viable stand-alone organization or should it be broken up and have its responsibilities merged into other parts of the Department of Homeland of Security such as CBP?

Answer. As you know, the Department looked at a variety of organizational issues as part of the second-stage review process, which helped clarify where the Department needs to be organizationally to ensure effective implementation of our critical missions. We considered whether ICE should remain a stand-alone entity, and decided that it should. We believe it's in the Department's best near and long-term interest that ICE not be merged with another component, CBP in particular. To reach this decision, we focused on the operational mission needs of both CBP and ICE, not on the near-term management challenges. I take seriously the challenges the Department has faced concerning ICE and appreciate the difficult but necessary choices Congress has made in providing new funding to address its needs. I am confident, however, that ICE has made substantial improvements in financial management this year. Not only have substantial new resources been provided, but a new management team is taking shape.

HOMELAND SECURE DATA NETWORK

Question. The fiscal year 2006 President's budget contains the first request to the Appropriations Committees regarding the Homeland Secure Data Network (HSDN). Why should funds be appropriated for HSDN now when the Department has seen fit to absorb $79 million in the past 2 years and not seek proper appropriated dollars for this purpose?

Answer. Anticipating the need to share intelligence and other information securely to fulfill its homeland security mission and to ensure efficient and effective use of scarce funds, the DHS CIO streamlined and merged disparate classified SECRET network initiatives within the Department into a single secure network called the Homeland Secure Data Network (HSDN). Existing agency funds for these initiatives were used to stand up this critical infrastructure. However, the fiscal year 2006 funding request is needed to use the additional funds to expand HSDN into a major, secure information thoroughfare joining together intelligence agencies, law enforcement, disaster management, and front-line disaster response organizations in the common goal of protecting our Nation and its citizens. An expanded HSDN will provide Secret connectivity and the required efficient information sharing capability to the non-DOD government community.

Question. Does DHS have the ability to share classified information today? If yes, why does a stand-alone system need to be built for DHS?

Answer. Today only a few Homeland Security components have the ability to share classified information over the DOD's SIPRNet. The present HSDN capabilities currently support over 30 DHS sites and will expand classified connectivity to

60 DHS sites in the next 2 months. DHS, and the non-DOD, government sector (including other Federal, State, local and tribal government) require the infrastructure and the processes and procedures to share classified information wholly effectively. The HSDN is an essential step that will allow the efficient sharing of classified information required for the mission of protecting the homeland. DOD policy in the wake of September 11, 2001, has been to migrate non-Defense, homeland security classified communications off SIPRNet and onto the HSDN. The DOD policy is based on the desire to ensure the SIPRNet can effectively support the war-fighting mission. DOD and DHS have established a joint, controlled interface between SIPRNet and DHS to provide for several levels on connection between HSDN and SIPRNet based on policy.

Question. Why isn't the budget for this project consolidated? Why is it being funded by specific organizations of the Department?

Answer. HSDN has rapidly evolved from an initially conceived agency specific network to a presently deploying DHS-wide network based on mission needs. HSDN is funded by charging each agency based upon the HSDN usage by that agency during a yearly time period. The working capital fund has served as a method to consolidate organizational element funding to support a single HSDN capability. The specific organization funding level will be adjusted as the usage requirements of each agency change over time.

Question. What is the rationale for how much each agency is being charged for HSDN?

Answer. The HSDN rationale for charging each agency is based upon the HSDN usage by each agency during a yearly time period. Presently, a formula has been developed that charges an agency based on its HSDN participation. Basically, this formula develops a percentage by agency based on the number of locations (sites) and the number of terminals (workstations) installed. The number of sites (large, medium and small) and seats is a usage-based cost model. Site size is an industry standard such applied by an internet service provider who charges are based on the size of your site (bandwidth of the connection). The usage is also determined by the number of seats. While some sites will allow multiple users for a single workstation, the number of seats sets the usage level at the site.

Question. The Information Analysis and Infrastructure Protection Directorate has in its budget the Information Sharing and Collaboration program. One of its responsibilities is "fostering collaboration among various levels of government and the private sector through the creation of a secure information sharing environment capitalizing on existing opportunities". How does this project relate to HSDN? Are these duplicative or complementary efforts?

Answer. These are complementary efforts. In May 2004, my predecessor, Secretary Ridge, created the Information Sharing and Collaboration (ISC) initiative to coordinate and facilitate efforts throughout the Department and with our customers and partners, particularly the Federal, State, tribal and local governments, and the private and international sectors, to affect change and improve information sharing and collaboration to secure the homeland. Since then, the importance of information sharing has been made more evident through the publication of numerous reports (such as the 9/11 Commission Report, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, and GAO studies), the issuance of new Executive Orders (for example, E.O. 13356), and a new public law, Public Law 108–458, the Intelligence Reform and Terrorism Prevention Act of 2004. Section 1016 calls for the creation of an Information Sharing Environment, which will require the sharing of information at levels including unclassified, sensitive but unclassified, SECRET, and perhaps higher.

Anticipating this need to share intelligence and other information securely to fulfill its homeland security mission, DHS is streamlining and merging disparate classified SECRET networks into a single, integrated network called HSDN. We envision that HSDN will become a major, secure information thoroughfare joining together intelligence agencies, law enforcement, disaster management, and front-line disaster response organizations in the common goal of protecting our Nation and its citizens. The ISC does not build systems or operate networks, such as the HSDN. The ISC initiative ensures system and network investments support DHS' information sharing mission.

OFFICE OF SCREENING COORDINATION AND OPERATIONS

Question. The President's budget proposes to create the Office of Screening Coordination and Operations, or SCO, within the Border and Transportation Security Directorate. How do you see this new office contributing to the Department's ability

to implement the 9/11 Commission recommendation regarding a comprehensive screening system with system-wide goals?

Answer. I support the concept of a Screening Coordination and Operations (SCO) Office, and developed plans through the 2SR process to meet the goals of the office. Consistent with the 9/11 Commission recommendations, HSPD–11 and HSPD–12, the SCO office will develop a more unified, comprehensive and efficient system for the screening, credentialing, and redress for passengers and leverage current investments in screening systems and tools. The SCO will harmonize IT architecture, uniform redress policies, and provide coordinated or shared services such as card production, biometric/biographic databases, as well as set DHS standards for information technology enterprise architecture and global enrollment systems/processes. The SCO office will develop a consistent approach for outreach in the areas of privacy, civil rights, and will coordinate R&D efforts. DHS will set up the SCO office in fiscal year 2006, as reflected in the Department's revised fiscal year 2006 request.

Question. Should the SCO have actual operational authority for various screening programs as proposed, or should it focus on the integration and coordination function, for example the development of the Department-wide credentialing standards necessary across so many programs involved in this activity?

Answer. I support the concept of a SCO Office, and developed plans, through the 2SR process, to meet the goals of the office. Consistent with the 9/11 Commission recommendations, HSPD–11 and HSPD–12, the SCO office will develop a more unified, comprehensive and efficient system for the screening, credentialing, and redress for passengers, while leveraging investments in screening systems and tools. The SCO will harmonize IT architecture, establish uniform redress procedures, and provide coordinated or shared services such as card production, biometric/biographic databases, common DHS standards for information technology architecture, and global enrollment systems/processes. The SCO office will develop a consistent approach for outreach in the areas of privacy, civil rights, and helping to ensure coordinated R&D efforts. DHS plans to set up the SCO office in fiscal year 2006.

Question. At the same time that significant programs are being proposed to be moved from Customs and Border Protection and the Transportation Security Administration, the President's budget does not propose moving the operational responsibility for any of the programs that incorporate screening of applicants out of U.S. Citizenship and Immigration Services (CIS). In order to ensure that there is the closest possible coordination across screening programs, should CIS screening programs also be moved to the SCO? Why wasn't CIS included?

Answer. I support the concept of a SCO Office, and developed plans through the 2SR process to meet the goals of the office. Consistent with the 9/11 Commission recommendations, HSPD–11 and HSPD–12, the SCO office will develop a more unified, comprehensive and efficient system for the screening, credentialing, and redress for passengers and leverage current investments in screening systems and tools. The SCO will harmonize IT architecture, uniform redress policies, and provide coordinated or shared services such as card production, biometric/biographic databases, as well as set DHS standards for information technology enterprise architecture and global enrollment systems/processes. The SCO office will develop a consistent approach for outreach in the areas of privacy, civil rights, and will coordinate R&D efforts. DHS will set up the SCO office in fiscal year 2006, as reflected in the Department's revised fiscal year 2006 request.

US VISIT

Question. How do you plan on addressing the issue of integration of the two fingerprint systems—IDENT at the Department of Homeland Security and IAFIS at the Federal Bureau of Investigation?

Answer. The US VISIT Program, working closely with CBP and ICE, and the Departments of Justice and State, leads the IDENT/IAFIS integration efforts. DHS' systems receive daily updates from the FBI with information from a variety of criminal and threat-related databases. There are several different ongoing efforts to bring about interoperability between the IDENT and IAFIS.

—DHS (US VISIT) established an integrated project team (IPT) with the FBI (Criminal Justice Information Services or CJIS) to address the policy, business requirements, and technical aspects of integrating IDENT and IAFIS. This IPT has made significant progress in resolving many of the long-standing issues in the DOJ Office of the Inspector General's report. A report, describing plans for interoperability, was submitted to Congress on August 18, 2005.

—Integrated IDENT/IAFIS workstations will be deployed to sites that will have US VISIT—115 airports, 15 seaports, and 165 land border ports of entry—as well as to specific ICE field office locations, by the end of calendar year 2005.

—DHS and DOJ have completed a Memorandum of Understanding (MOU) to resolve data access and privacy issues concerning FBI usage of US VISIT data.

Question. Are there any DHS/FBI jurisdiction issues hampering the integration effort?

Answer. DHS and DOJ/FBI have achieved an effective working relationship on integration. As noted above, DHS (US VISIT) and FBI (Criminal Justice Information Services or CJIS) have established an integrated project team (IPT) to address the policy, business requirements, and technical aspects of integrating IDENT and IAFIS. This IPT has made significant progress in resolving many of the long-standing issues originally referenced by the DOJ Office of the Inspector General. A report, describing plans for interoperability, was submitted to Congress on August 18, 2005.

GLOBAL SUPPLY CHAIN SECURITY

Question. Mr. Secretary, in your written testimony you used cargo container security as an example of an area where the Department could do a better job coordinating across all departmental efforts. What impact have the various programs the Department is running had on cargo container security so far? What can be done better?

Answer. Since September 11, 2001, the various cargo security programs now operated by the Department have made great strides in moving us towards a system of security that prevents the use of the supply chain in a terrorist attack while enhancing supply chain efficiency and reliability. Before September 11, most cargo security efforts were centered at the port and based on local perceptions of risk. Today we have improved data reporting through the 24 Hour Rule supported by centralized targeting at National Targeting Center. This capability coupled with the Container Security Initiative has allowed us to revolutionize the customs function by allowing us to interdict threats before they leave for the United States.

Our current programs and capabilities have laid the foundation for a truly 21st century international trade system, one that will support growth in international trade and our security interests. Other efforts, such as Operation Safe Commerce, the Advanced Container Security Device program and the Advance Trade Data Initiative, will provide us with the knowledge and tools to help us get there. To that end, I am reviewing the status of DHS's cargo security efforts, how they can be further strengthened and how we can further transform the system to ensure the United States security and economic needs are met.

Question. What is the status of the final report on Operation Safe Commerce, and when will it be submitted to this Committee?

Answer. The report on Operation Safe Commerce (OSC) requires submission of program information from OSC's three participating load centers. One participant's input was behind schedule but has recently been received. This information will be integrated into a report and distributed for review by relevant experts. We expect the report to be issued by the end of December 2005.

Question. What more should be done in this area?

Answer. I am reviewing the status of DHS's cargo security efforts, how they can be further strengthened and how we can further transform the system to ensure the United States security and economic needs are met.

AGRICULTURAL INSPECTIONS

Question. The April 14, 2005, U.S. Department of Agriculture, Office of Inspector General Report regarding coordination between the Department of Homeland Security and the Department of Agriculture indicates that coordination has been less than adequate for the last 2 years. Specifically, the report mentions APHIS personnel being denied entry to ports-of-entry to conduct its required regulatory reviews. What are you doing to change this situation?

Answer. CBP and the U.S. Department of Agriculture (USDA) Animal and Plant Health Inspection Service (APHIS) signed in February 2005 Appendix 8 to Article 8 of the Memorandum of Agreement (MOA) between DHS and the USDA. The MOA establishes and enhances coordinated actions and operations between the two agencies and responds to many of the issues raised in the Office of Inspector General (OIG) report.

CBP and USDA APHIS have forged a new working relationship and resolved many of the earlier port access issues. CBP, in conjunction with APHIS, has entered into several programs, such as the targeted program for imported cut flowers to apply inspection resources on a risk managed basis (i.e., focus on commodities that pose a higher risk to American Agriculture). Also, CBP and APHIS have worked together in numerous ways to synchronize and verify information and data collected

about inspections such as the Joint Quality Assurance Program, which provides a quality assurance team to conduct port reviews. CBP and USDA employees are working together cooperatively and sharing information. CBP has worked with USDA to achieve the appropriate level of access to the ports of entry for APHIS personnel. As Congress has provided, the inspectional functions were transferred from USDA to CBP. CBP has set forth procedures that have facilitated USDA access to the ports to perform their functions.

Question. The OIG report includes information of the lengthy time that was required to negotiate and sign official agreements between APHIS and Customs and Border Protection (CBP). Several of these have taken more than 12 months. Additionally, APHIS reported that attempting to elevate issues within the Department of Homeland Security was not productive due to high turnover in the policy-making levels of DHS. The Homeland Security Act of 2002 split the agriculture responsibilities between these two agencies. If this is not working, should this situation be reevaluated?

Answer. Section 421 of the Homeland Security Act of 2002 (the Act) transferred to DHS the inspectional functions of APHIS relating to agricultural import and entry inspection. By the provisions of the Act, the Secretary of USDA and the Secretary of DHS were required to execute a memorandum of understanding (MOU) to cover this transfer in more detail. The MOU was signed on February 28, 2003.

Under the provisions of the MOU, the two agencies would work out further details of this relationship by the means of appendices to particular articles in order to allow for the development of procedures that would work for both agencies. To date CBP and APHIS have signed appendices to all the articles except for Article 4 that involves training in order to allow for the development of procedures that would work for both agencies. The time spent in developing the correct procedures has been well worth the delay as the training functions between the two agencies are working effectively. A completed Appendix for Article 4 is expected to be signed in early summer 2005.

We have also developed procedures and mechanisms to work through issues as they arise in the future. The time taken to draft, negotiate and finalize these appendices has been a necessary part of a growing partnership between these two agencies. The organizational and functional task allocations are working. The agricultural program is being strengthened through training and cross training.

NATIONAL PREPAREDNESS GOAL

Question. The Administration released the Interim National Preparedness Goal (the Goal) on March 31, 2005. States are required to update their State Homeland Security Strategies, by October 1, 2005, with an assessment of what gaps remain in each state's ability to meet the tasks and capabilities laid out in the Goal. The proposal put forth by the fiscal year 2006 President's budget would prioritize Federal funding received by State and local governments for first responders not just by threat and vulnerability, but also by "essential capabilities" as defined in the Goal. Each State is required to file an addendum by October 1, 2005, to its State Homeland Security Strategy to reflect how it will address the seven national priorities. Is this enough time for the States to do a thorough evaluation of what capabilities each has now?

Answer. Yes, DHS believes that there is enough time for the States to complete a thorough evaluation of their current capabilities. Specifically, in fiscal year 2005, during year 1 of the implementation of Homeland Security Presidential Directive (HSPD) 8, States and urban areas are required to update their existing homeland security strategies. To meet this requirement, the Department is asking States and urban areas to review their existing strategic goals and objectives and bring them into alignment with the seven National Priorities outlined in the National Preparedness Goal by September 30, 2005. (The seven National Priorities are: (1) Implement the National Incident Management System and National Response Plan; (2) Expand Regional Collaboration; (3) Implement the Interim National Infrastructure Protection Plan; (4) Strengthen Information Sharing and Collaboration Capabilities; (5) Strengthen Interoperable Communications Capabilities; (6) Strengthen CBRNE Detection, Response, and Decontamination Capabilities; and (7) Strengthen Medical Surge and Mass Prophylaxis Capabilities.) This first step in HSPD–8 implementation will not require States or urban areas to conduct a wholesale rewrite of their strategies, nor will they have to complete another risk and capabilities assessment as they did in fiscal year 2003. DHS completed guidance on completing this strategy in June 2005. More detailed information on this requirement was presented to State and urban area representatives at three National Preparedness Goal rollout conferences throughout April and May 2005. Additional details are also available to

State and urban area representatives through their designated Preparedness Officers within the Office for Domestic Preparedness (ODP) in the DHS Office of State and Local Government Coordination and Preparedness (OSLGCP).

Question. An important aspect of the National Preparedness Goal has not been defined, the levels of capabilities for differently sized jurisdictions. How are Manchester, NH, and New York, NY, supposed to know what different types of capabilities that each should have for a chemical incident?

Answer. The Interim National Preparedness Goal establishes the national vision and priorities that will guide DHS' efforts, in conjunction with appropriate stakeholders, to set measurable readiness benchmarks and targets to strengthen the Nation's preparedness. The Target Capabilities List is a set of 36 essential capabilities that should be developed and maintained, in whole or in part, by various levels of government to prevent, protect against, respond to, and recover from terrorist attacks and major disasters. DHS, working with stakeholders, is currently developing national target levels for the capabilities and the role of Federal agencies, states, local jurisdictions, the private sector and non-governmental organizations in building and maintaining the network of capabilities across the country required for large-scale incidents. Local jurisdictions will be expected to build and maintain levels of capability appropriate to their risk. DHS has invited Federal agencies, State representatives, and national associations to participate in a series of workshops to set the target levels.

Question. How will you encourage States to be thorough in their assessment of their capabilities?

Answer. In out-year implementation of HSPD–8, States will be required to assess their current capabilities against target levels of capability that will be defined in the Target Capabilities List. However, in fiscal year 2005, the capability assessment will be conducted through a representative sampling of States and/or sub-state regions to test and validate the assessment process prior to nationwide implementation. As part of this representative sampling of capabilities, DHS will develop user-friendly tools based on the Target Capabilities List to ensure that both States and multi-disciplinary subject-matter expert teams conducting the assessments are thorough in their evaluation of capabilities. In addition, DHS will provide customized reports to States that link their existing capabilities and grant expenditure data to the National Priorities outlined in the National Preparedness Goal in order to assist States as they begin to implement HSPD–8.

Question. What is the incentive for a State to close a gap if doing so results in less funding for that State?

Answer. The Department believes there are sufficient incentives for States to build both regional and statewide capabilities and close identified gaps in overall preparedness. Enhanced preparedness to protect against, respond to, and recover from incidents of a national emergency, including terrorism, will ultimately result in minimizing the adverse impact on lives, property, and the economy that are inherent to a catastrophic event. The protection of citizens, critical infrastructure, businesses, and communities is a shared goal, requiring Federal, State, local, international, and private sector partnerships. Throughout the Nation, States are embracing this goal as the ultimate incentive, as they work to implement the National Preparedness Goal. Finally, the extent of "unmet gaps" will not be the sole determinant of DHS grant allocations.

Question. How exactly does the Administration envision this working?

Answer. The Interim National Preparedness Goal includes a vision, which is "to engage Federal, State, local, and tribal entities, their private and non-governmental partners, and the general public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and the economy."

The Interim National Preparedness Goal and companion National Preparedness Guidance outline how the Nation will achieve this vision. The Guidance outlines a 10-step national process for Capabilities-Based Planning that will be used to identify target levels of capability, achieve them, and assess preparedness from the local to the national level. The Goal and Guidance establish seven National Priorities focused on developing some of the more critical capabilities from the Target Capabilities List for which the Nation is currently the least prepared (Information Sharing and Collaboration; Interoperable Communications; Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Detection, Response, and Decontamination; and Medical Surge and Mass Prophylaxis) and overarching initiatives (to implement the National Incident Management System, National Response Plan, Interim National Infrastructure Protection Plan, and expand regional collaboration) that will facilitate those efforts. The Guidance highlights existing Federal program efforts that support the seven National Priorities and describes a schedule of activities for

States and urban areas to update assessments and strategies with Federal assistance.

The process is collaborative, iterative, and risk-based. Homeland security is a shared responsibility and depends upon shared efforts. This approach will be implemented through multi-agency and multi-discipline working groups at the national and regional (or multi-jurisdiction) level. Federal preparedness assistance will explore ways to offer incentives and rewards for collaboration. This approach involves a continuous cycle of activity to refine our assumptions and planning tools and share best practices and lessons learned. This approach recognizes that while all jurisdictions are subject to some degree of risk, the capabilities and levels of capability that are needed to manage risk vary considerably across the Nation. Annual status reports will provide a more meaningful assessment of national preparedness. Data collection will simplify over time as tools are refined and consolidated. This approach will provide a sound basis for decisions at all levels of government to allocate resources based upon risk and need.

Question. Will "essential capabilities" as defined by the National Preparedness Goal be considered equal to threat information, population density, or other factors?

Answer. The development of the target capabilities, or "essential capabilities," by Federal, State, local, and tribal entities and the private sector will be driven by relevant threat information, population size and density, critical infrastructure, and other factors. DHS is working with Federal, State, local, tribal, private sector, and non-governmental stakeholders to refine the Target Capabilities List (TCL) for reissuance on October 1, 2005. This new version of the TCL will assign the capabilities by level of government and tiers (groupings of local jurisdictions). The primary purpose of the tiers is to account for reasonable differences in target levels of capability (or system-specific elements of capability) among groups of jurisdictions based on differences in risk factors such as total population, population density, and critical infrastructure.

Question. Once a State obtains certain capabilities, how do we sustain that effort? Should the States be responsible for sustainment costs?

Answer. As we have barely begun to assess current capabilities, it is premature to speculate about future funding requirements once the most significant gaps are closed. While maintenance of effort will largely be State and local responsibility, DHS will continue to assist States in building and sustaining the target capabilities. Additionally, every State and locality will have a role in achieving and sustaining the 36 capability target levels. However, the target capabilities are a planning tool, not a funding formula. Implementing Capabilities-Based Planning is a long-term effort that will help the Nation to achieve the capacity to perform all 36 target capabilities at the levels needed to effectively prevent, protect against, respond to, and recover from major events, especially terrorism. Not until States and urban areas have assessed and realigned their homeland security strategies and plans will DHS be able to fully determine which of the 36 target capabilities will require additional funding.

FUNDING FOR FIRST RESPONDERS

Question. Just in the last few weeks national news reports have questioned the use of first responder grants in relation to homeland security. In January of 2005, the Department of Homeland Security Office of Inspector General issued a report questioning how the Department prioritized port security grants.

Given all of this, how confident are you that every dollar that has been allocated for homeland security grants has been well spent?

Answer. In general, homeland security port security grants have been well spent. Recognizing that issues emerged with some projects, the Department disagreed and non-concurred with the IG's finding that projects received funding despite ranking "average to worse" during the evaluation process. Following TSA's second round of grant awards in 2003, ODP made $75 million available for port security grants under the Urban Areas Security Initiative (UASI). ODP, in consultation with TSA and SLGCP, utilized a risk-based approach, which differed from the program's original competitive process to select 14 eligible port areas and the corresponding funding amounts for each area. TSA then provided unfunded applications from its second round to ODP, which in turn, funded 86 projects. TSA provided what they considered to be the next projects that had been evaluated from the previous round that deserved funding. All of the 86 projects were funded based on TSA's recommendations.

The Department has made significant efforts to improve the Port Security Grant Program in light of the Inspector General's (IG) report. The report recommended that the Department accelerate the acquisition of more information from applicants

about the scope of their projects in an effort to expedite the spending of grant awards. We concur with this recommendation and will ensure that appropriate guidance on the submission of relevant information within specified timeframes is included in the application kit for the forthcoming fiscal year 2005 Port Security Grant Program. Additionally, the IG report recommended that the Department ensure that the program has sufficient operational expertise to administer the program after the award is made. We concur with this recommendation as well, and have established a Transportation Infrastructure Security Division (TISD) within SLGCP to administer the fiscal year 2005 Port Security Grant Program. Given the reforms in response to the IG report, DHS port security grants will be managed even more effectively under the fiscal year 2005 Port Security Grant Program. Additionally, SLGCP has developed mechanisms intended to increase accountability of all grant programs, an effort recognized in a recent GAO Report entitled, "Management of First Responder Grants Has Improved, but Challenges Remain" (#05–121).

Question. The Senate and the House Appropriations Committees asked for a report on homeland security grant spending. This report is to include information on what has been purchased with all of the grant dollars from fiscal years 2002 through 2004, whether these purchases complied with the State Homeland Security Strategies, and an explanation as to how this spending has enhanced the Nation's security. That report was due March 31, 2005, but it has not yet been submitted. When can we expect it?

Answer. The congressional report on "State and Local Government Preparedness and Funding for Fiscal Year 2002-Fiscal Year 2004" was delivered to the House and Senate Appropriations Committees on May 6, 2005.

Question. If the Department goes to a completely threat-based formula, are you comfortable with how threats are determined now? I know we can't talk in detail in an open forum—but what, if anything, would you change?

Answer. The President's fiscal year 2006 Budget proposes a risk-based homeland security funding process, of which threat is one component along with consequence and vulnerabilities. DHS will consider risk factors such as threat, presence of critical infrastructure, vulnerability, population and population density, international borders, and ports of entry in making final award determinations. This process will be modeled on the fiscal year 2005 UASI program, which combined five variables designed to objectively prioritize funding for high-threat, high density urban areas. A threat estimate index developed from an estimate of credible threats and incidents as well as an index that considered law enforcement investigative activity and enforcement will be used. The difficulty of determining which States and urban areas most are at risk is subjective to some degree because of the nature of most intelligence information and the scarcity of data specifically identifying targeted states, cities and infrastructure. Therefore, the current allocation methodologies that consider threat information represent the best available combination of data, current understanding of threats, and expert judgment.

Question. What restrictions are placed on the use of these grant funds?

Answer. DHS released detailed guidance for the use of grant funds contained in the fiscal year 2005 Homeland Security Grant Program (HSGP). Specific guidelines on intended purpose and the allowance of certain types of expenditures vary between the six different programs contained in the HSGP. HSGP allowable costs are divided into planning, organization, equipment, training, and exercise categories. Management and administrative and certain operational costs are also allowed under certain programs. Allowable equipment categories for the fiscal year 2005 HSGP are listed on a web-based Authorized Equipment List on the Responder Knowledge Base, which is sponsored by ODP and the Oklahoma City National Memorial Institute for the Prevention of Terrorism at http://www.rkb.mipt.org.

The fiscal year 2005 HSGP guidance also details certain restrictions placed on the use of grant funds, which vary by program. For example, funding in the UASI and Law Enforcement Terrorism Prevention Program programs may not be used for overtime to supplant ongoing, routine public safety activities of State and local emergency responders, and may not be used to hire staff for operational activities or backfill. However, these programs do allow up to 25 percent of the awards to be used for operational expenses and overtime for periods of heightened alert, for personnel to participate in information, investigative and intelligence sharing activities related to homeland security, and finally, in the hiring of contractors/consultants for participation in information/intelligence sharing groups. Another example of restriction on funds involves construction and renovation. Use of HSGP funds for construction is generally prohibited and is allowable only when it is a necessary component of (1) a security system at critical infrastructure facilities or (2) an emergency operations center (EOC). Details on other restrictions for certain types of equipment, training, and exercises are provided in the fiscal year 2005 HSGP guidance.

Question. What audits have been done, or are underway, to ensure that these grant funds are used appropriately? What other controls does the Department have at its disposal to oversee the use of grant funds?

Answer. During calendar year 2004, SLGCP was a part of over 14 governmental audits, ranging from the Government Accountability Office (GAO) to the DHS Inspector General to the House Appropriations Survey & Investigations Staff (S&I). Many of these audits looked at the expenditure of grant funds by the States and territories. Some of these audits have provided final reports, and most of those reports reflect SLGCP's ability to efficiently process the grant, as well as provide programmatic assistance and oversight to the states. A recent GAO Report entitled, "Management of First Responder Grants Has Improved, but Challenges Remain" (#05–121) credits SLGCP with developing requirements intended to hold States and localities accountable for how grant expenditures were planned, justified, expended, and tracked.

In order to assure fiscal and programmatic oversight, ODP Preparedness Officers have robust monitoring and reporting tools through which they can monitor expenditures by grantees. The Initial Strategy Implementation Plan and the Biannual Strategy Implementation Report provide detailed expenditure information by discipline, solution area (such as equipment or training) and project area. These reports require grantees to tie any expenditure of homeland security funds to goals and objectives outlined in their State or Urban Area Homeland Security Strategy. They also provide important data on what projects are being accomplished by States and localities. In addition to the almost daily contact with grantees, Preparedness Officers also perform a formal on-site monitoring visit to their States at least once a year, in accordance with program office protocols. This visit allows for both programmatic and financial compliance monitoring. The Department of Justice's Office of the Comptroller (OC) also performs random, risk-based financial audits of SLGCP grantees. Each State Administrative Agency (SAA) also is subject to its own State audits. The combination of these external and internal inspections provides the required oversight over the use of SLGCP grant funds.

INTEROPERABLE COMMUNICATIONS

Question. The Federal Government has been working for many years to crack the nut of moving more quickly towards true interoperability. Do you see the creation of the Office of Interoperability and Compatibility as helping move towards that goal? Is this just another Office that will put forth a lot of effort and get very little advancement?

Answer. The Science and Technology (S&T) Directorate's Office for Interoperability and Compatibility (OIC) has made significant achievements in helping the Federal Government move more quickly towards interoperability. The OIC was created to address critical interoperability issues relating to public safety and emergency response, including communications (the SAFECOM Program), equipment, training and other areas as needs are identified.

Since its inception OIC has:

—Released Version 1.0 of the first ever comprehensive Public Safety Statement of Requirements (SoR) for Communications and Interoperability (SoR), which defines the functional requirements for public safety practitioners to communicate and share information when needed, where needed, and when authorized.

—Developed the Interoperability Continuum, a tool designed to help the public safety community and local, tribal, State, and Federal policy makers address critical elements for success as they plan and implement interoperability solutions. The critical elements include governance, standard operating procedures, technology, training/exercises, and usage of interoperable communications.

—Created the Statewide Communications Interoperability Planning (SCIP) Methodology, based on lessons learned from assisting the Commonwealth of Virginia in developing a strategic plan for improving statewide communications interoperability. The SCIP Methodology serves as a guide for States to consider as they initiate statewide communications planning efforts.

—Developed coordinated grant guidance which provides the public safety community with consistent guidance, coordinated application processes, similar requirements across grant programs, and general guidelines for implementing a successful wireless communications system. This guidance was incorporated in the fiscal year 2003 FEMA and fiscal year 2003/fiscal year 2004 Community Oriented Policing Services (COPS) grant awards, as well as ODP grant packages in fiscal year 2004.

—Drafted a report as required by the Intelligence Reform and Terrorism Prevention Act that discusses DHS plans for accelerating voluntary consensus standards for interoperable communications.
—Managed the RapidCom initiative, in which the Office worked with ten urban areas to provide requested assistance to help improve incident level interoperability capabilities and developed a methodology for a communications table top exercise that is replicable across urban areas.
—Awarded a contract to develop and execute the nationwide interoperability baseline study in January 2005. The purpose of the study is to quantify the extent to which the Nation's public safety first responders are interoperable technically and operationally.

With respect to other critical interoperability issues, the OIC has done the following:

—Created the Risk Assessment Policy Group (RAP) from representatives within DHS to address and resolve discrepancies in risk assessment criteria and methodologies. RAP hosted a workshop with stakeholders from the Department to clearly define the scope of the risk assessment problem and to develop a strategy for addressing the problem.
—Created the Joint Evaluation and Testing Program (JET) to coordinate Federal programs that conduct testing and evaluation of public safety technologies. JET hosted a planning meeting with representatives from DHS, the National Institute of Standards and Technology, and the Department of Justice to define the scope of the JET program.

Question. The Office of State and Local Government Coordination and Preparedness reports that in fiscal year 2004 more than $890 million of the grants given to States and locals were used in some way for interoperable communications, equipment, studies, etc. What is being done to help States and locals today to make better decision about investments in interoperable communications?

Answer. SLGCP has leveraged the S&T Directorate's SAFECOM program's development of standards and grant guidance to help create the Interoperable Communication Technical Assistance Program (ICTAP). ICTAP is a technical assistance program designed to enhance interoperable communications between local, State, and Federal emergency responders and public safety officials. The goal of the ICTAP program is to enable local public safety agencies to communicate as they prevent or respond to a WMD attack. The ICTAP program provides free, on-site support using a systems engineering approach. The ICTAP technical assistance team works closely with the UASI site's Urban Area Working Group to assess the current communications infrastructure for gaps and to translate operational requirements into technical requirements that can be used to design an interoperable communications system.

AIR CARGO SECURITY

Question. Does the Transportation Security Administration (TSA) have any cost estimates for screening 100 percent of the baggage and cargo on passenger planes?

Answer. The total amount of cargo transported on passenger aircraft represents less than 25 percent of the total air cargo volume transported in the United States. TSA completed a study in 2002, "The Air Cargo Security Scenario Analysis Report," that indicated that the cost of screening 100 percent of the cargo transported on passenger aircraft at the top 42 airports, which handle 95 percent of the total volume of air cargo transported in the United States, would cost $500 million in the first year and $3.8 billion over 10 years.

Question. Though you cannot deter every threat, do you believe 100 percent screening of high-threat of bags and cargo is the best use of our Federal resources?

Answer. TSA has taken a threat-based, risk-managed approach to air cargo screening. This approach helps the agency appropriately target screening efforts with the resources available. TSA believes that all cargo should be pre-screened for risk through the Known Shipper Program or the Indirect Air Carrier Program, and that 100 percent of cargo that is identified as elevated-risk should be screened using appropriate technology and methods. Random inspections play an important, complementary role in the layered systems approach by managing risk without unduly impeding the flow of commerce.

Currently all cargo that will be transported on passenger aircraft is pre-screened for risk through the Known Shipper Program. Passenger air carriers, Indirect Air Carriers (IACs, or freight forwarders), and all-cargo carriers who transfer cargo to passenger planes all use the Known Shipper Program. TSA's Known Shipper Database has centralized the collection of data on about 450,000 known shippers and enabled vetting against government databases. To supplement the Known Shipper

pre-screening, air carriers are also required to conduct random screening of a certain percentage of air cargo.

In 2005, TSA has developed an Air Cargo Security Roadmap that integrates many policy, operations, system, and regulatory enhancements to air cargo security. The cornerstone of this effort is the Freight Assessment System (FAS), which would enable TSA to better and more efficiently identify elevated-risk cargo for inspection. FAS will employ a sophisticated risk assessment engine to identify elevated-risk air cargo for inspection.

Additionally, TSA has published a robust Notice of Proposed Rulemaking (NPRM) for air cargo security. This NPRM is currently being developed into a final rule, which implements major security enhancements for indirect air carriers (IACs), all cargo carriers, passenger carriers, and airports.

Finally, TSA oversees compliance with security requirements through a robust regulatory compliance program, which includes more than 900 aviation security inspectors located throughout the United States.

Question. How can we better tackle the issue of cargo security?

Answer. TSA continues to make incremental and measured progress in the air cargo arena, among other things by prohibiting cargo from unknown shippers, significantly increasing the number of physical inspections of air cargo on passenger and all cargo aircraft, increasing its air cargo inspections workforce, strengthening the criteria for consideration as a known shipper, automating the validation of known shippers and indirect air carriers, and expediting research and development efforts to identify potential new technological solutions for the inspection of air cargo on passenger aircraft. TSA is also working closely with CBP to develop a targeting tool which will permit effective identification of elevated risk cargo with the ultimate goal of requiring the inspection of all such elevated risk cargo.

Question. What is the right mix of screeners and technology when dealing with air cargo and how does the Department determine which resources to apply?

Answer. TSA has taken a threat-based, risk-managed approach to air cargo screening. This approach helps the agency appropriately target screening efforts with the resources available. TSA believes that all cargo should be pre-screened for risk through the Known Shipper Program or the Indirect Air Carrier Program, and that 100 percent of cargo that is identified as elevated-risk should be screened using appropriate technology and methods. Random inspections play an important, complementary role in the layered systems approach by managing risk without unduly impeding the flow of commerce.

TSA employees do not conduct the screening of air cargo. Rather, the screening is performed by air carriers and overseen by TSA. TSA issues regulatory requirements to air carriers in this area, and TSA's inspectors provide oversight and work to ensure that carriers are meeting their regulatory requirements.

Question. What other means is TSA using to achieve more secure cargo-holds in passenger carriers?

Answer. TSA is continuing efforts to design blast resistant cabin and cargo liners, as well as overhead bin mitigation technological solutions. The agency has completed initial feasibility studies for both passenger cabin and cargo hold liners. The results of the studies are promising. The agency is working on preliminary designs, and a prototype is expected by the end of calendar year 2005. TSA is also partnering with the FAA and aircraft manufacturers to determine which solutions are best suited for retrofitting existing aircraft with this new technology.

Additionally, TSA is conducting a pilot program to evaluate the use of blast-resistant containers for cargo and baggage on passenger aircraft to fulfill the requirements of Section 4051 of Public Law 108–458, the Intelligence Reform and Terrorism Prevention Act. The objective of the hardened unit load device (HULD) pilot program is to determine the feasibility, including operational impact, durability, cost, maintenance, training, blast containment, and logistics, of an HULD solution. The pilot program began in June 2005, and the data collection will last approximately 18 months from the start date.

Question. How difficult is it for TSA to secure the air cargo processing "footprint" at the airports from the time of entry into the system maintaining a chain of custody until the moment of its loading onto a plane?

Answer. Regulated airports already secure their air cargo processing "footprint" through security measures specified within their airport security program which identifies a portion of the airport as Secured Area, Security Identification Display Area, and Sterile Area. These security procedures are designed to prevent unauthorized entry, presence, and movement of individuals and ground vehicles within the air operations area. Current procedures require a personnel identification system which allows different levels of access, subjects individuals to employment history verification checks, and provides individual training.

Question. What are other countries doing to address this issue?

Answer. The United Nations' International Civil Aviation Organization (ICAO) establishes International Standards, Recommended Practices and Procedures covering the technical fields of aviation, including air cargo security.

Countries or States, as commonly referred to by ICAO, are afforded a great deal of discretion to establish and implement measures to comply with standards directly related to air cargo security. The substance of ICAO's air cargo standards are as follows:

—States shall ensure the implementation of measures at airports serving international civil aviation to protect cargo and baggage moved within an airport and intended for carriage on an aircraft to safeguard such aircraft against an act of unlawful interference.

—States shall establish measures to ensure that cargo intended for carriage on passenger flights are subjected to appropriate security controls.

—States shall establish measures to ensure that operators do not accept consignment of cargo for carriage on passenger flights unless the security of such consignments is accounted for by a regulated agent or such consignments are subjected to other security controls.

The ICAO Security Manual provides guidance on how an ICAO Member State might comply with the standards. The methods of compliance provided in the guidance material are based on generally recognized practices and procedures common within the international civil aviation industry, but they are not the only means of compliance. ICAO recognizes that other methods of compliance may be equally appropriate.

TSA PASSENGER FEES

Question. The President's budget request proposes increasing the passenger security fee by $3.00 from $2.50 to $5.50 for the first leg of an airline trip. Has TSA or the Department conducted any studies to determine what the flying public would pay in exchange for better aviation security?

Answer. Yes. The Aviation and Transportation Security Act (ATSA), enacted in November 2001, anticipated that the aviation industry, not the general taxpayer, would pay for airline security costs. To estimate the passengers' willingness to pay the additional cost of air transportation, TSA conducted an analysis that included comparing year-to-year revenue collections, reviewing Department of Transportation data reported by the airlines themselves to estimate industry growth, utilizing the Federal Aviation Administration's (FAA) aviation industry forecast, and accessing major research studies that outline issues from airline fare structure to passenger demand and willingness to pay.

TSA also conducted a review of current research on air passengers' willingness to pay for aviation security. Of particular interest to TSA was a survey conducted by the National Opinion Research Corporation in August 2002 of airline passengers for the American Automobile Association (AAA). In that survey, approximately nine out of ten respondents indicated that they were willing to pay something more than the current passenger security fees. AAA's conclusion is as follows: "Americans remain committed to aviation security. It's one thing to demand increased security and to be unwilling to pay for it. No one likes to pay more for the goods or services we buy. But what this survey seems to say is that Americans not only want to feel secure when they fly, they are willing to pick up some of the cost, if necessary."

Question. What is the impact to the industry?

Answer. TSA believes that the modest fee increases of this proposed budget should not undermine passenger traffic nor worsen the industry's health. U.S. air traffic reported for 2004 by the Department of Transportation (DOT) is near or above the year 2000 levels. Despite the re-imposition of fees after a 4 month suspension under the Emergency Wartime Supplemental Appropriations Act, 2003 (Public Law 108–11), the DOT domestic passenger traffic statistics showed an increase from a total of 588 million in 2003 to 630 million in 2004—a 7.2 percent increase.

TSA researched the impact the fee increase might have on airline profitability. TSA was unable to locate any study that conclusively linked a passenger fee increase, applicable to all airlines, with a measurable decline in airline profitability. The September 11 Security Fee is a uniform fee imposed on the passengers of all similar air carrier operations and flights. Consequently, the fee should not put individual airlines in a competitive disadvantage with one another. In fact, the security and other aviation fees comprise a larger percentage of the ticket price for low cost carriers, yet the low cost carriers are currently the most profitable among the domestic airlines.

TSA regularly monitors the state of the aviation industry, including the level of operations and the financial status of the airlines. Here are two examples of informational sources TSA uses in order to accomplish this goal:

—Various publications of the DOT Airline Fares Consumer Report were analyzed, and it was found that the answer depends upon various factors such as market size, number of carriers, and market structure. The data shows that competition within the aviation industry has a stronger influence on base fares than security fees.

—Canada has extensively researched the economic impact of its passenger security fee called Air Travelers Security Charge. Using both Canadian and U.S. data, the researchers concluded that markets with traffic levels over 100,000 passengers are relatively price inelastic (an increase in price results in either no or virtually no reduction in demand.). The research results did not find that the September 11 Security Fee impacts airline profitability.

Question. Does the passenger fee proposal require legislation or are there other options?

Answer. The passenger security service fees were authorized by the Aviation and Transportation Security Act and codified at 49 U.S.C. 44940. Currently, 49 U.S.C. 44940(c) limits the passenger fee to $2.50 per enplanement, not to exceed $5 per one-way trip. The proposal to increase the passenger fee would require 49 U.S.C. 44940(c) to be modified to set the new fee level at $5.50 per enplanement, not to exceed $8 per one-way trip.

Question. The budget requests that this fee change be legislated on an appropriations bill. However, this should properly be submitted to the authorizing committees of jurisdiction. Has the President transmitted the proposed legislation to Congress for consideration and if not, why?

Answer. The President provided a legislative proposal to modify this fee authority in the fiscal year 2006 budget. In Title V—General Provisions of the Appendix (page 526), the proposal states: "SEC. 517. In Chapter 449 of title 49, United States Code, section 44940(c) is amended by striking '$2.50' and replacing it with '$5.50', and striking '$5.00' and replacing it with '$8.00'." This modification to the fee authority would allow TSA to implement the fee increases sought in the President's fiscal year 2006 Budget.

Question. What will be the impact on DHS' programs and activities if this legislative proposal is not enacted as a general provision of the Appropriations Act or by the appropriate authorizing committee?

Answer. The sharing of aviation screening costs between industry, passengers, and Government is essential to ensure that there is sufficient funding for existing and emerging threats to the integrity of the aviation security infrastructure. The proposed increase is intended to shift the burden of paying aviation screening services from the general taxpayer to the airline passenger. The Department will work with Congress to ensure that security priorities are met.

Question. When would such a fee request have to be enacted to fund fiscal year 2006 activities?

Answer. TSA estimates that if the fee were to be enacted in time to be effective at the beginning of fiscal year 2006, the agency will be able to raise as much as $1.879 billion in additional fees. If the proposal is enacted after October 1, the delay involved in providing the necessary updates in fees and guidance to the industry could result in reduced collections.

Question. What new aviation security measures would you put in place utilizing the increased revenues or will these resources be used throughout the Department?

Answer. The purpose of the fee increase is not to fund new activities. Rather, it is to offset funding from the general fund with fee revenue. Compared to the past and current level of 50 percent or less, the fee would contribute to offsetting nearly the full amount of TSA screening costs.

These costs represent the vast majority of TSA's aviation security screening costs. TSA does not have the authority to offset any other costs with the aviation security fee collections. The increased fees on passengers, the users of the security screening, will ensure fee levels approaching near full recovery of the Federal cost to operate the system.

TSA AIR CARRIER SECURITY FEES

Question. At the direction of the Committee, GAO has completed a review in order to validate the air carrier's estimates of their security costs in 2000. GAO found that the estimates, currently the foundation for the fees paid to the Department by the airlines, are $127 million too low. Due to these findings, Mr. Secretary, will you take action to collect the additional fees from the airlines?

Answer. In the Homeland Security Appropriations Act, 2005, (Public Law 108–334) Congress directed the GAO to determine how much air carriers spent on security screening in 2000—the basis for the fee imposed on airlines. GAO completed its review and issued a report on April 18, 2005. The report concludes that the amount of the industry-wide passenger and property screening costs was between $425 million and $471 million, with a midpoint estimate of $448 million. The midpoint difference between what is collected now and what GAO indicates should be collected is $129 million. However, GAO's estimate did not include certain cost categories (e.g.; real estate, CAPPS, and positive bag match) due to the unavailability of information within the timeframe provided. The cost of these items could be significant. TSA is currently reviewing all the findings of the. Once TSA completes its review, the agency will proceed as quickly as practicable to address the issue.

Question. Will TSA require legislation to change the air carriers' charges or can this be done through regulation?

Answer. No legislation is required. The fiscal year 2005 Homeland Security Appropriations Act and the Aviation and Transportation Security Act, as codified at 49 U.S.C. 44940, provide sufficient authority for TSA to collect additional amounts from the air carriers. However, changes to the air carriers' fees would require changes to regulations currently in effect at 49 CFR Part 1511.

Question. When must the regulation be in place in order to generate enough revenues to cover your costs in fiscal year 2006?

Answer. To collect the air carrier fee at the current level of approximately $315 million in fiscal year 2006, no new or changes in the regulation would be required. The $350 million estimated in the President's budget captures costs that are currently disputed or not reported altogether by air carriers due to bankruptcies. TSA is in the process of pursuing the amounts under dispute. The unreported and disputed costs will be determined and charged when TSA implements the new structure for the air carrier fee, for which rulemaking is currently in progress. Additionally, TSA is currently reviewing GAO's findings that the aviation security costs self-reported by the air carriers should be $448 million, $129 million more than originally reported by the industry.

Question. Will your regulatory proposal focus on changing the basic structure of how airlines are charged for security costs or is it intended to focus on the difference between the actual revenue generated, $350 million, and TSA's target last year of $750 million?

Answer. TSA is evaluating the current regulatory approach to determining if change is needed.

Question. For fiscal year 2005, there are some that estimate the air carrier fee will generate only $315 million, not $350 million. What are you planning to do to address any shortfall?

Answer. The $315 million represents a total rounded year 2000 cost figure reported by all carriers to TSA. The $350 million estimate captures costs that are currently disputed or not reported altogether by air carriers due to bankruptcies. TSA is in the process of pursuing the amounts under dispute. The unreported and disputed costs will be determined and charged when TSA implements the structure for the air carrier fee, for which rulemaking is currently in progress.

Question. What activities will go unfunded or deferred as a result of the funding gap?

Answer. The sharing of aviation screening costs between industry, passengers, and Government is essential to ensure that there is sufficient funding for existing and emerging threats to the integrity of the aviation security infrastructure. The proposed increase is intended to shift the burden of paying aviation screening services from the general taxpayer to the airline passenger. The Department will work with Congress to ensure that security priorities are met.

TSA CONTRACT SCREENERS

Question. What analysis has the Department done to determine whether contracting for private screeners is cost-effective and equally or more effective in terms of security than a federalized force?

Answer. TSA commissioned an independent evaluation of the five pilot airport passenger screening programs that was completed in April 2004. The evaluation utilized a methodology that included the following:

Evaluation Categories:

—Security effectiveness: covert test results, Threat Image Protection (TIP), and re-certification scores;

—Customer/stakeholder satisfaction: customer surveys, stakeholder surveys, and customer complaints; and

—Cost: total cost the contractor charged for screening services (including only contract payments and costs borne by TSA) compared to estimates on how much would have been spent by TSA had the agency conducted the screening operations at those airports.

The evaluation concluded that there was no statistical difference in any of the three evaluation categories between private and Federal screeners. In addition, as more airports transition to the Screener Partnership Program (SPP), TSA plans to continue to measure costs of Federal screening operations compared to private screening companies.

TSA also commissioned an activity-based cost (ABC) study to provide improved visibility into the costs of specific business processes and activities, and the associated resources (e.g., people, technology) consumed by those processes and activities (i.e., cost per bag or person screened). The ABC study included ten randomly selected airports that utilize TSA screeners and the five pilot airports. The study will better enable TSA to identify and collect the cost and performance metrics needed to establish a successful, ongoing cost and performance management framework at TSA. The results of the ABC study will provide another means for TSA management to assess screening operations by airport.

Question. Is TSA establishing a cost benchmark and collecting the right kind of information in order to evaluate the costs of providing Federal screeners vs. the costs of having contract screeners?

Answer. TSA plans to develop a cost baseline for each airport that applies to participate in the SPP. This cost baseline will be used to evaluate cost proposals from private screening companies. The results of the TSA activity-based cost study will also support development of these baselines.

Question. In what ways is it more effective for the government to use contract screeners?

Answer. An independent evaluation concluded that there was no statistical difference between private and Federal screeners. TSA believes that the independent evaluation, along with the activity-based cost study, confirms that TSA has been successful in administering an effective private screening program that is capable of providing security screening services at levels required by the ATSA.

Question. What incentives do you have in place and what are you doing to address the private sector's concerns about security liability related to the private screener workforce?

Answer. In directing TSA to establish a contract screening pilot program (PP5), the ATSA required that the level of screening services and protection provided at the PP5 airports be equal to or greater than the level provided at an airport with Federal screeners. Consequently, as airports consider whether to continue with Federal screening or to apply to the SPP, their decisions can be based on their own preferences and criteria rather than considerations of security, resources, or level of service.

ATSA states that TSA shall allow an airport operator to submit an application to have screening carried out by the screening personnel of a qualified private screening company. TSA is committed to developing a fair, balanced program that does the following:

—Meets ATSA standards
—Ensures security
—Seeks to establish a strong public/private partnership
—Provides significant opportunity for innovation, efficiency, and cost savings to the taxpayer
—Provides decentralized management
—Incorporates best practices and lessons learned from recent studies of the Pilot program, and continues to evaluate and learn on an on-going basis
—Is performance-based
—Does not restrict airport participation
—Respects Federal and private sector workforces

Under ATSA, the decision to apply for private screening services lies with individual airport operators. However, should TSA approve the application, TSA will continue to oversee airport security, whether an airport has private contract screeners or Federal screeners.

TSA does not provide specific liability limitations for private passenger and baggage screening services. However, vendors can apply for protections under the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act). Enacted as part of the Homeland Security Act of 2002, the SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by creating a system of risk and liability management. The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers/sellers from mak-

ing anti-terrorism technologies available. The Act provides two types of benefits: (1) Designation as a Qualified Anti-Terrorism Technology ("QATT"), which among other benefits limits the seller's liability to the amount of available insurance, and (2) Certification as an Approved Product for Homeland Security, which allows the seller to assert the Government Contractor Defense. Sellers must apply for SAFETY Act protections and are evaluated in accordance with the statutory criteria. Protections under the SAFETY Act only apply when a QATT has been deployed in defense against, response to, or recovery from an act of terrorism. The Act contains a very broad definition of technology, which includes both tangible products and services as long as they designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring act of terrorism.

TSA is working with the S&T Directorate, which is charged with making determinations regarding the SAFETY Act. TSA understands that two of the private contract screening companies under the PP5 program have been granted designation under the SAFETY Act. TSA will also continue to work closely with DHS and the S&T Directorate regarding any decision DHS makes concerning the potential legal exposure of all entities participating in the Screening Partnership Program.

Question. How well have the privatized screeners at the 5 pilot airports worked?

Answer. TSA believes that private screeners and Federal screeners perform equally as well in screening passengers.

Question. A recent article in Government Security News reports that the traveling public is more satisfied with the private screeners than the Federal screeners. Is this an accurate statement?

Answer. This is not an accurate statement. TSA's annual customer service survey showed that for the second year in a row there was very little difference in the high degree of confidence and satisfaction air travelers have in TSA-trained screeners—Federal or private. For the second year in a row, air travelers gave consistently high marks to TSA's security screeners. Between 80 and 95 percent of passengers gave positive responses when asked about seven aspects of the Federal security screening process, which included thoroughness and courtesy of screeners as well as confidence in TSA's ability to keep air travel secure. In addition, TSA is meeting or exceeding passenger expectations for security line wait times.

Question. This past November TSA opened the Program Management Office to assist airports in privatizing their screener workforce. How many applications for private screeners has this office received?

Answer. As of May 2005, TSA has received seven applications from airport operators seeking to participate in the SPP. All five of the airports that participated in the private screening pilot program (PP5) have applied (San Francisco, Kansas City, Rochester, Jackson Hole, and Tupelo), along with two new airports (Elko, Nevada and Sioux Falls, South Dakota).

Question. How many applications for private screeners at airports do you anticipate receiving?

Answer. The decision on whether to apply to the SPP rests solely with the airport. Therefore, although several airports have expressed interest in participating in the program, TSA cannot speculate on how many will actually apply.

Question. How did you determine the level of screening service to be provided at these 5 airports?

Answer. The ATSA requires that the level of screening services and protection provided at the PP5 airports be equal to or greater than the level provided at an airport with Federal screeners. TSA will continue to set one standard for security for the entire commercial aviation system, whether an airport has Federal screeners or private screeners. TSA will ensure that standards are met through TSA security protocols, extensive contract oversight, conducting covert testing, and continuous oversight by Federal Security Directors and their staff in both Federal and SPP airports.

Per ATSA, TSA is also required to supervise private screening services at each SPP airport. Private screeners must perform at the same or better level as Federal screeners and comply with Federal passenger and baggage screening standard operating procedures.

ATSA also gives TSA the ability to terminate a contract with a private screening firm for repeatedly failing to perform. TSA will not hesitate to take action against airports using contract screeners if they fall below Federal security standards, and TSA will vigorously enforce the contract requirements.

Question. Are the screening standards for the privatized airports negotiated or does TSA establish them?

Answer. TSA applies the same rigorous security standards, referred to officially as Standard Operating Procedures, to private screeners as it does to the Federal screeners. Passenger and baggage security screening standards are non-negotiable.

Question. Does the contract include paying for the annual recertification of screeners by the contractor as well as compensation and benefits?

Answer. Yes. Screener annual re-certification training is conducted by and paid for by TSA. Private screener compensation and benefits are also funded by TSA up to the point required by the ATSA which mandates that private screeners receive compensation and benefits are not less than the compensation and benefits for Federal screeners.

Question. Does the private screener workforce have access to Federal benefits or is this just strictly a contract for services provided?

Answer. No, private screener workforce employees do not have access to Federal benefits. While the ATSA mandates that private screeners receive compensation and benefits that are not less than the compensation and benefits for Federal screeners, those benefits are not provided by the Federal Government. Screeners employed by private screening companies do receive benefits, and TSA monitors the overall pay and benefits package provided by private screening companies to ensure that the ATSA-mandated minimum is attained.

Question. What changes would you recommend to the contract screener program?

Answer. At the present time, TSA is not seeking changes to the ATSA regarding provisions to this program. TSA is open to and welcomes dialogue with airports and Congress on any improvements that could be made to the SPP. Some of the changes airports have indicated that they would like to see include the following:

—Change ATSA's requirement that private screening compensation and benefits be equal to or greater than Federal compensation and benefits

—Allow airports to share in any savings realized. For example, cost savings realized at an airport with private screeners would be used to enhance security screening at that airport

—Investigate pooling worker's compensation insurance to reduce costs through economies of scale

—Investigate broadening the private screening contractor's scope of responsibility to include other non-screening functions that impact security screening (e.g., document checkers, baggage handlers, bin runners, equipment maintenance, etc.)

TSA SCREENER TRAINING

Question. How many hours of training does the average screener receive?

Answer. The ATSA requires that all screeners complete a minimum of 40 hours of classroom training and 60 hours of On-the-Job (OJT) training. In addition to this basic training requirement, TSA Federal Security Directors (FSD) also use a standard of 3 hours per week (measured on average over a calendar quarter) of scheduled duty time, per screener, to accomplish recurrent, administrative, and professional development training. The FSD must create a training schedule that meets the goal of the 3 hours per week standard as well as the specific performance and developmental needs of each individual screener. In addition, TSA provides screeners with additional skills directly related to specific screener duties. An example is the On-screen Alarm Resolution Protocol (OSARP) Training. OSARP allows screeners to evaluate items causing an alarm and to potentially clear those items without subjecting the bag to a secondary search. The training for OSARP totals 19.5 hours and includes classroom training, small group simulator training, hands-on individual simulator training, and OJT training.

Question. Who conducts the training?

Answer. Basic screener training is overseen by TSA's Office of Workforce Performance and Training (WPT). The training is provided by instructors under contract with TSA or by local TSA Approved Instructors (TAIs) when possible. On-the-Job, cross-over, recurrent, and specialized training is conducted by local TSA personnel (i.e., TAIs, Training Coordinators, Screener Supervisors) and via the Online Learning Center. Advanced training is initially provided by WPT contractors and then sustained by TAIs.

Question. Does this training include anything regarding ethics and baggage theft?

Answer. During the initial 100 hours of basic training, TSA requires all screeners to review and sign a Code of Conduct. This Code of Conduct emphasizes such issues as public trust and honesty. Once initially trained, screeners continually receive recurrent professional ethics training including the "Customer Service Web-Based Training," which reinforces TSA's customer service principles and gives the screener training in various scenarios requiring effective customer service responses. Screeners are also provided the "TSA Pledge to Travelers," which emphasizes TSA's dual mission of providing World Class Security and World Class Customer Service, assures the traveling public that they are entitled to a security screening experience

that is professional and courteous, and that any experience to the contrary should be reported back to TSA. In addition, TSA has sent several communications to all employees (not just screeners) of their responsibilities on ethical conduct, including the restrictions under the Hatch Act related to the acceptance of gifts by Federal employees. All employees also receive a copy of and are required to sign TSA HRM Letter No. 735–1, Interim Policy on Employee Responsibilities and Conduct, which contains many of the Standards of Conduct provisions. Finally, to remind screeners of the consequences of unethical behavior, TSA has disseminated Management Directive 1100.75–3 informing screeners of the policies and procedures for disciplinary actions that could be taken against them.

TSA is committed to providing comprehensive ethics training and is currently developing a general ethics course that is expected to be available via the Online Learning Center by the end of the third quarter of fiscal year 2005. This course will cover topics such as principles, misuse of position, gifts, and outside activities.

Question. What is your response to the OIG's report regarding baggage theft by screeners?

Answer. TSA's responses to the specific recommendations in the Inspector General's report are as follows:

Recommendation 1.—Evaluate the adequacy of supervision, the physical layout of inspection stations, and the feasibility of installing electronic surveillance techniques near inspection stations.

TSA continuously reviews procedures related to the screening of baggage including supervision of personnel, physical layout, and electronic surveillance techniques. The agency will continue to do so by implementing the congressional requirements of the Intelligence Reform and Terrorism Prevention Act concerning checked baggage screening area monitoring, which requires the Under Secretary for Border and Transportation Security to provide assistance, subject to the availability of funds, to public airports that have baggage handling areas that are not open to public view in the acquisition and installment of security monitoring cameras for surveillance of such areas in order to detect theft from checked baggage and to aid in the speedy resolution of liability claims against TSA.

TSA's Office of Aviation Security Programs is working closely with the Office of the Chief Information Officer to plan and execute a program for the installation of electronic surveillance systems (ESS) to deter and detect incidents of baggage pilferage and claims arising from such incidents. $14 million has been made available for ESS systems in fiscal year 2005 and plans are being developed to either install ESS where none existed before or make use of or supplement existing airport systems to leverage available resources. TSA is working in partnership with airports to find the most cost effective means to install and maintain current and future ESS systems.

Searching checked baggage in view of the passenger obviously mitigates incidents of pilferage, but as inspection stations move away from lobbies and into airport baggage handling areas, ESS will rise in importance as will emphasis on proper supervision of such areas.

Recommendation 2.—Include a module on professional ethics in its screening training curriculum.

A general ethics course is under development and should be available on the Online Learning Center in the next 4–6 weeks. This course will be mandatory for all TSA employees, with a second component required for all supervisors available during the same timeframe. New employees will have 90 days to complete this course. For existing employees, the training will be required within 6 months.

On pages six and seven of the draft report, there is discussion of previous cases of prosecution against TSA screeners based on "sting" or surveillance evidence. The Office of Workforce Performance and Training will incorporate the occurrence of such incidents into an existing lesson that is currently taught in all three of the basic screener training courses (Dual Function Screener, Passenger, and Baggage).

Currently, TSA screeners do receive some ethics training though they are not required to receive annual ethics training because they do not file financial disclosure reports. The field attorneys at the Office of Chief Counsel often make annual ethics training sessions for financial disclosure filers at their airports available to the screener workforce as well. TSA screeners received the TSA Guide to Major Ethics Rules as new employees. Also, all employees must sign the TSA HRM Letter No. 735–1, Interim Policy on Employee Responsibilities and Conduct, which contains many of the Standards of Ethical Conduct provisions. Field attorneys have also displayed ethics posters in TSA offices and breakrooms.

Additionally, in 2003 and 2004, several articles in The Sentinel were published on ethics issues, including the 14 Principles of Ethical Conduct, gifts, buddy passes,

and the Hatch Act. The Sentinel is a newsletter distributed to the entire TSA workforce.

Recommendation 3.—Resume negotiating an agreement with the airline industry on shared liability for lost or stolen baggage claims.

TSA recently resumed discussions with the airline industry based on the following set of objectives: (1) improve customer service, including communication to the passengers about where to file claims; (2) enhance detection of fraud, including duplicative claims; (3) facilitate cooperation in resolving exceptional claims when necessary; and (4) develop open channels of communication between the Claims Management Office and airline claims offices.

At a meeting on January 11, 2005, the airlines were receptive to these proposed goals, and TSA provided a white paper to the airline community describing our proposed goals in June 2005. The airline associations will then share this paper with their members and provide feedback to TSA. The goal is to have a memorandum of cooperation that all domestic airlines are able to sign by late summer 2005.

General Comment to the Report.—The topic of property inadvertently left out of bags is discussed on page 7 of the OIG report. TSA recognizes that this is a problem and has advised that this property be handled as lost and unclaimed property. Under lost and unclaimed procedures, property recovered after checked baggage has been screened will be inventoried and held for at least 30 days to provide the owner an opportunity to reclaim the property. Should it be unfeasible or impractical for the owner to reclaim the property in a timely fashion, and he or she has evidence that TSA opened his or her baggage through such means as a Notice of Inspection, the passenger may submit a claim for the missing property.

Question. How do you track a screener's progress in terms of consistently utilizing the skills and delivering the appropriate and acceptable service and security they've been trained to deliver?

Answer. As mandated in a February 2004 TSA Management Directive, all training accomplishments must be documented in TSA's centralized Online Learning Center (OLC). TSA management routinely monitors compliance with mandatory training requirements and recurrent training guidelines. Federal Security Directors (FSD) are responsible for ensuring compliance locally on an individual basis.

The aforementioned management directive has been updated as part of the routine annual review cycle and was circulated for comment within TSA in May 2005. This update includes clear language on the responsibility of the training administrator to document all required training within 30 days (7 days for screener basic training), the supervisor's responsibility to ensure their employees have completed all required training, and the role of the course sponsor to monitor national compliance with program requirements. TSA intends to ensure that all employees complete the required amount of training by incorporating this requirement into the fiscal year 2006 Performance Agreements of all TSA supervisors.

In May 2005, the OLC was enhanced to include a much more robust reporting engine that will provide Training Administrators and Course Sponsors with detailed accountability reports.

Additionally, screeners must undergo re-certification each year. The re-certification program for 2004–2005 includes three separate paths: passenger, dual function, and baggage. Passenger screeners must pass three modules. Module 1 is a job knowledge, Standard Operating Procedures (SOP)-specific test. Module 2 is an image test. Module 3 contains practical skills demonstrations. Dual function screeners take both job knowledge tests for passenger and baggage screeners, an image test, and practical skills demonstrations. Baggage screeners must pass two modules, a job knowledge, SOP-specific test and practical skills demonstrations.

To be re-certified, screeners have to pass all applicable modules of the Knowledge and Skills Assessment Program and achieve a rating of meets or exceeds' standards on their annual Personal Performance Assessment. Screeners are afforded one opportunity for remediation and retest. Following a retest, those screeners who fail to re-certify are terminated.

Question. How do you hold the screeners accountable for inappropriate behavior?

Answer. The responsibility and accountability for employee conduct issues rests with the Federal Security Directors at airports. TSA has implemented a leadership model that requires managers to address behaviors that fail to support the TSA mission and to work with employees to engage in appropriate behaviors or face consequences for continued patterns of misconduct. TSA has also implemented policies to implement single step termination procedures for high-risk offenses such as illegal drug use, alcohol on duty, and theft. TSA regards the commission of such offenses as posing a potential security risk. TSA is always mindful of ensuring that due process protections for employees are maintained and has appropriate appeal mechanisms for conduct matters to include the Disciplinary Review Board, the

Agency Grievance process and appeals to the Office of Civil Rights. In addition, TSA has a Professional Review Board at headquarters to review and take appropriate action for misconduct involving senior level employees.

Question. What are the penalties for poor performance?

Answer. The penalties for poor performance range from counseling to removal depending upon the nature, cause, and severity of the performance deficiency. Additionally, screeners must undergo re-certification each year. Failure to re-certify may result in termination or, in special cases, retraining.

Question. In the worst case what is the threshold for removal from work?

Answer. TSA has established mandatory termination procedures for offenses such as illegal drug use, alcohol on duty, and theft. TSA regards the commission of such offenses as posing a potential security risk. In addition, TSA has established policies for first offense terminations for matters affecting integrity and security at the airport such as sleeping on duty, violations of Standard Operating Procedures, security breaches, and criminal conduct.

Question. With such a high workmen's compensation number—one of the highest of the Federal workforce—is there specialized training in place to address this?

Answer. In early fiscal year 2003, TSA met Congressional deadlines to hire Federal airport passenger screeners and achieve checked baggage screening using Explosive Detection Systems. As the TSA screening workforce was deployed, it became apparent that injuries caused by lifting and quickly moving baggage were a serious problem. TSA initiated a safety program in the second quarter of fiscal year 2003 to address the high rate of injuries.

Fiscal year 2004's rate increase from fiscal year 2003 is attributed, in part, to the processing of backlogged claims from incidents that actually occurred in fiscal year 2003. In fiscal year 2004, TSA began implementation of an Occupational Safety and Health program aimed at lowering TSA's injury and illness rate. By the midpoint of fiscal year 2004, a decrease in the number of claims could be seen, and the decrease appears to be continuing into fiscal year 2005. Training, guidance, a nurse intervention program, and the availability of field safety support have contributed significantly to the decrease. For example, in the first 15 weeks of operation, the nurse intervention program at 21 pilot airports yielded savings of over $2.2 million.

It is important to emphasize that airline baggage handling is among the most injury prone occupations in the private sector. TSA is committed to the well-being of its employees and is taking the steps necessary to reduce screener injuries by improving working conditions and appropriately managing the claims process.

TSA has also distributed a safety awareness Web-Based Training (WBT) course both as a CD and via the Online Learning Center. This safety awareness WBT course covers such topics as proper lifting techniques, heat injury prevention, and checkpoint and checked baggage safety. In addition, training on radiation safety awareness is being developed.

TSA "NO FLY" LISTS/SECURE FLIGHT

Question. How does one get on the "no fly list", and more importantly, how does someone get off the list?

Answer. U.S. Government intelligence and law enforcement agencies collect, analyze, and evaluate data used to nominate subjects to the No-Fly List. Intelligence analysts and law enforcement officers within these organizations carefully review nominations based on the No-Fly List criteria and thoroughly evaluate the information during each step of the process. Watch List nominations often contain classified and/or sensitive law enforcement investigative information. Nominations that meet the established criteria are forwarded to the National Counterterrorism Center (NCTC) and the Terrorist Screening Center for inclusion in the TSC Data Base (TSDB) and for addition to the No-Fly List. Time sensitive nominations may be routed directly to the TSC if required.

If it is determined that a person on the No-Fly List should no longer be identified as a No-Fly subject, they will be removed from the list. If additional intelligence data is developed or a subject has been interviewed by U.S. Government officials and deemed no longer a threat, an official request for removal must be submitted to the agency that placed the individual on the list. The original nominating agency will evaluate the data and determine whether the person stays on or is removed from the No-Fly List. The nominating agency will then make a formal request through the nomination chain requesting that the person be removed from the No-Fly List. In some cases, a review of the derogatory information associated with a No-Fly nomination may result in the subject being downgraded to the TSA Selectee List.

The TSA Office of Transportation Security Redress is currently developing a redress process for addressing any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening under the future Secure Flight program. This process will also allow passengers who feel they have been erroneously placed on the watch lists to undergo a case review. TSA will work with the nominating agency to review the derogatory information. The redress process will be coordinated with other DHS redress processes as appropriate.

TSA has developed and implemented a clearance protocol for persons who are flagged for additional screening due to the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA will review the submission and reach a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. The Passenger Identify Verification Form, as well as other information, has been posted on TSA's public website at the following web address: http://www.tsa.gov/public/display?theme=157&content=09000519800fb8af

However, this clearance process will not remove a name from the watch lists. Instead, this process distinguishes legitimate passengers from persons who are on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Following TSA-required identity verification procedures, airline personnel can then quickly determine that these passengers are not the person of interest whose name is actually on the watch lists.

In addition, an individual may seek to challenge his or her inclusion on a watch list in a court of competent jurisdiction after the redress and appeals process within TSA has been exhausted.

Question. What is TSA doing to address the fact that people are erroneously placed on the list or have mistaken identities?

Answer. TSA has developed and implemented a clearance protocol for persons who are flagged for additional screening due to the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA will review the submission and reach a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. The Passenger Identify Verification Form, as well as other information, has been posted on TSA's public website at the following web address: http://www.tsa.gov/public/display?theme=157&content=09000519800fb8af

However, this clearance process will not remove a name from the watch lists. Instead, this process distinguishes legitimate passengers from persons who are on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Following TSA-required identity verification procedures, airline personnel can then quickly determine that these passengers are not the person of interest whose name is actually on the watch lists.

In addition, an individual may seek to challenge his or her inclusion on a watch list in a court of competent jurisdiction after the redress and appeals process within TSA has been exhausted.

The TSA Office of Transportation Security Redress is currently developing a redress process for addressing any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening under the future Secure Flight program. This process will also allow passengers who feel they have erroneously been placed on the watch lists to undergo a case review. TSA will work with the nominating agency to review the derogatory information.

Question. What's the appeal process for these people? Is it within or outside TSA?

Answer. TSA has developed and implemented a clearance protocol for persons who are flagged for additional screening due to the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA will review the submission and reach a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. The Passenger Identify Verification Form, as well as other information, has been posted on TSA's public website at the following web address: http://www.tsa.gov/public/display?theme=157&content=09000519800fb8af

However, this clearance process will not remove a name from the watch lists. Instead, this process distinguishes legitimate passengers from persons who are on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Following TSA-required identity verification procedures, airline personnel can then quickly determine that

these passengers are not the person of interest whose name is actually on the watch lists.

In addition, an individual may seek to challenge his or her inclusion on a watch list in a court of competent jurisdiction after the redress and appeals process within TSA has been exhausted.

Question. Is there legal recourse for those mistakenly put on the list?

Answer. The TSA Office of Transportation Security Redress is currently developing a redress process for addressing any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening under the future Secure Flight program. This process will also allow passengers who feel they have erroneously been placed on the watch lists to undergo a case review. TSA will work with the nominating agency to review the derogatory information.

Question. What is the Department doing to address the serious concerns about privacy and the use of personal passenger information?

Answer. To protect passengers' personal information and civil liberties, TSA and the Secure Flight program will:

—Limit the collection of personal information to only what conforms to the relevant and necessary standard according to The Privacy Act of 1974 (5 U.S.C. 552 (a));
—Limit access to the information to only those TSA employees and contractors who have a "need to know" clearance in order to perform their duties associated with Secure Flight operations;
—Ensure that each employee and contractor associated with the Secure Flight program has completed the TSA mandatory privacy training prior to beginning work on the program;
—Limit sharing of personal information to the Federal Bureau of Investigation (FBI) and intelligence agencies that need the information for investigatory purposes related to aviation security, in accordance with TSA's Privacy Act System of Records Notice published for the program;
—Include a built-in auditing mechanism to detect unauthorized access to the personal information stored for the program;
—Limit the retention of the data. TSA has requested that the National Archives and Records Administration approve a 72-hour retention period for the information collected and used for the Secure Flight program unless a longer retention period is requested by the passenger for redress; and
—Include robust redress mechanisms to enable passengers to work with TSA to resolve instances in which they think they are being inappropriately selected for secondary screening or they are having a difficult time obtaining boarding passes.

Question. TSA has a program under development, called Secure Flight which takes personal passenger information and compares it to the "no fly list" in an effort to identify suspected terrorists traveling by air. How do you respond to concerns raised by both the DHS OIG and the GAO about the Department's handling and use of the personal passenger information related to Secure Flight? What are you doing to remedy the situation?

Answer. To protect passengers' personal information and civil liberties, TSA and the Secure Flight program will:

—Limit the collection of personal information to only what conforms to the relevant and necessary standard according to The Privacy Act of 1974 (5 U.S.C. 552 (a));
—Limit access to the information to only those TSA employees and contractors who have a "need to know" clearance in order to perform their duties associated with Secure Flight operations;
—Ensure that each employee and contractor associated with the Secure Flight program has completed the TSA mandatory privacy training prior to beginning work on the program;
—Limit sharing of personal information to the FBI and intelligence agencies that need the information for investigatory purposes related to aviation security, in accordance with TSA's Privacy Act System of Records Notice published for the program;
—Include a built-in auditing mechanism to detect unauthorized access to the personal information stored for the program;
—Limit the retention of the data. TSA has requested that the National Archives and Records Administration approve a 72-hour retention period for the information collected and used for the Secure Flight program unless a longer retention period is requested by the passenger for redress; and
—Include robust redress mechanisms to enable passengers to work with TSA to resolve instances in which they think they are being inappropriately selected for

secondary screening or they are having a difficult time obtaining boarding passes.

Question. Why did you discontinue development of Secure Flight's predecessor CAPPS II?

Answer. On September 24, 2004, DHS announced its intent to implement a next generation aviation passenger pre-screening program called Secure Flight. Unlike CAPPS II, Secure Flight will focus only on identifying potential terrorist threats (those people on watch lists) and, if a decision is made to use commercial data, it will be utilized in a focused and limited manner. Under Secure Flight, TSA will take over from the air carriers responsibility for the comparison of domestic airline Passenger Name Record (PNR) information against terrorist watch lists. Secure Flight will meet DHS' goals of improving the security and safety of travelers on domestic flights, reducing passenger airport screening time, and protecting privacy and civil liberties. Consistent with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), TSA will begin implementing Secure Flight in August 2005.

TSA recently concluded initial system effectiveness testing for Secure Flight. The commercial data testing began on March 18, 2005, and preliminary test results for the commercial data testing are expected later in 2005.

Secure Flight is designed to improve the efficiency of the prescreening process and reduce the number of people selected for secondary screening. TSA will compare domestic flight PNR information against records contained in the consolidated watch lists contained in the Terrorist Screening Data Base (TSDB), including the expanded No Fly and Selectee lists. Consolidating these checks within the Federal Government will allow TSA to automate most watch list comparisons and apply more consistent, internal analytical procedures when automated resolution of initial "hits" is not possible. Secure Flight will help eliminate false positive watch list matches, improve passengers' experience under the existing system by helping move passengers through airport screening more quickly, reduce the number of individuals selected for secondary screening, and allow for more consistent response procedures at airports for those passengers identified as potential matches. Consequently, TSA will be able to concentrate its screening resources more efficiently.

Finally, Secure Flight will only pre-screen travelers on domestic flights, while CBP will continue to vet passengers on international flights.

AIR TRAVELER SATISFACTION

Question. TSA is one of DHS' most visible agencies since they interact with the air traveling public on a daily basis. What is the most common complaint TSA receives?

Answer. TSA captures complaints reported at airports using TSA's web-based Performance Measurement Information System (PMIS). In April 2005, the most common complaint recorded by TSA's PMIS was the addition of butane lighters to TSA's Prohibited Items List, which was required by IRTPA (Public Law 108–458), Section 4025.

The most common complaint currently received by the TSA Contact Center (TCC) and recorded in the Inquiry Management System (IMS) involves the delays passengers experience during the airport check-in process as a result of having a name similar to, or the same as, individuals who are on a Federal watch list.

Question. Recently, TSA completed a customer satisfaction survey, what did it find?

Answer. The TSA developed the Customer Satisfaction Index for Aviation (CSI–A), which is a performance measure of our aviation screening program. The CSI–A score represents the customer satisfaction response based on a scale of zero to 100 percent where zero represents "very dissatisfied" and 100 percent represents "very satisfied". The CSI–A provides customer service and maintains public confidence while maintaining a high level of security. There are three components of the CSI–A: passenger surveys conducted at airports, national poll results conducted by the Bureau of Transportation Statistics (BTS), and complaints and compliments received by TSA.

The CSI–A score for fiscal year 2005 is 79 percent. The following scores reflect the breakout of each component:

—Passenger surveys conducted at airports=79 percent
—National poll results=75 percent
—Trend of complaints and compliments received by TSA=no significant change in trends
—The change in trends indicate the changes in feedback (complaint and compliments) received by TSA via the Performance Measurement Information Sys-

tem and the TSA Call Center. The aforementioned trend indicated the changes in feedback against time for fiscal year 2004.

Highlights of the 2005 passenger satisfaction survey are as follows:

—91 percent of passengers were satisfied with their overall experience at the passenger checkpoint;

—89 percent of passengers thought security was adequate, as opposed to excessive; and

—82 percent of passengers have confidence in TSA's ability to keep air travel secure.

Question. What other means are you using to validate the customer feedback findings of the survey?

Answer. TSA collects customer feedback on a daily basis. Customers have two means through which to provide feedback on their experience—providing the feedback while at the airport or contacting the TCC. Feedback received at airports is recorded using the web-based system known as the PMIS. PMIS enables TSA personnel at airports to record the feedback received from customers on a daily basis. In addition, PMIS offers airports the ability to record the number of compliments and complaints received according to a variety of categories. The categories are the same as those used by the TCC. Examples of categories include, but are not limited to: discourteous treatment, slow processing, and improper handling of property. This data in addition to the data from the TCC contributes to one of the three components of the Customer Satisfaction Index for Aviation.

Question. What role does the TSA Contact Center play regarding customer service?

Answer. The TCC serves as TSA's central customer service point of contact for all non-media public inquiries. These inquiries can be made to the TCC via telephone, facsimile, correspondence, and e-mail. The inquiries usually take the form of compliments, complaints, or requests for information on a particular issue or problem. For example, an individual may have a question regarding whether a particular item is prohibited in either checked or carry-on luggage and the Customer Service Representative (CSR) or agent will respond accordingly. If an individual has a complaint, the CSR will either attempt to resolve the matter or, if appropriate, refer the matter to a Customer Support and Quality Improvement Manager at the airport for appropriate action and follow-up with that individual. In addition, given the nature of the contact, a matter may need to be elevated to TCC management and/or referred to a program office within TSA for assistance. Furthermore, based on investigation or analysis of complaints and inquiries made to the TCC, recommendations are made to improve agency policies, procedures and practices.

The TCC also performs a security role in protecting the Nation's transportation systems. For example, the TCC forwards to TSA's Transportation Security Operations Center (TSOC) any communications or contacts mentioning, referencing, or alleging threats or security vulnerabilities. The TSOC will then take appropriate action to resolve the issue.

Question. What progress and improvements has TSA made using both the survey and the Center's feedback?

Answer. All feedback received by the passengers is used to make management decisions. Trend analyses, such as review of the top three complaints, are provided and reviewed by senior leadership on a monthly basis. Specific issues that are the result of recent policy changes are also addressed, such as recent complaints on pat-down searches and the amended Prohibited Items List. TSA headquarters is also rolling out a pilot program at ten airports to test a standardized customer comment card. The card is designed to provide a means for convenient and quick feedback at the airport level.

Question. How do you respond to the recent Government Security News article that passengers prefer private screeners' treatment of the passengers being screened?

Answer. The TSA annual customer service survey showed that for the second year in a row there was very little difference in the high degree of confidence and satisfaction air travelers have in TSA-trained screeners—Federal or private. For the second year in a row, air travelers gave consistently high marks to TSA's security screeners. Between 80 and 95 percent of passengers gave positive responses when asked about seven aspects of the Federal security screening process, which included thoroughness and courtesy of screeners as well as confidence in TSA's ability to keep air travel secure. In addition, on average TSA is meeting or exceeding passenger expectations for security line wait times.

Question. How are your wait times and your wait time web page working for TSA?

Answer. TSA continually seeks to evaluate and understand factors that increase wait times and how our service and staffing models can decrease wait times and

improve the screening process for passengers. All airports collect and report wait time data each hour of each day and on the half hour during peak hours of the day. This allows TSA to monitor the customer experience in order to ensure the traveling public is not overburdened with lengthy wait times while not compromising security. The wait time data is used to make improvements to checkpoint configurations and appropriate staffing levels.

Since collection of wait time data, the national average wait time has decreased to less than three minutes. Similarly, the average wait time during peak periods has decreased by almost four minutes since January 2004.

Month	Nationwide average wait time	Nationwide average peak wait time
January 2004	3.35 minutes	14.0 minutes
April 2005	2.95 minutes	10.1 minutes

In addition to using wait time internally to assist in identifying areas for improvement, TSA posts the wait time data on a public internet site available to travelers and the media. The URL can be found at http://waittime.tsa.dhs.gov/index.html. The web site provides the traveling public rolling average wait time by hour, by airport checkpoint, and by day of the week.

Question. What recourse do complainants have?

Answer. The recourse for complainants varies depending on the nature of the complaint. In the majority of cases, the matter is resolved by the Customer Service Representative (CSR) or agent who initially handles the inquiry by providing the individual with information as to why a particular action was taken or about processes currently in place. For example, in some cases, a TSA representative explains the redress process, usually used with claims or watch list issues, and provides the necessary forms. Unusual or less common complaints may need to be elevated to management and/or referred to the appropriate program office. This process ensures that TSA responds in a timely manner to inquiries received, while at the same time giving proper attention to any new trends or issues concerning TSA services. When an issue involves a particular airport, TSA refers the issue to a Customer Support and Quality Improvement Manager at the airport for appropriate action and follow-up with the complainant. The TSA Contact Center (TCC) is another vital tool and serves as TSA's central customer service point of contact for all non-media public inquiries. TSA headquarters is rolling out a pilot program at ten airports to test a standardized customer comment card. The card is designed to provide a means for convenient and quick feedback at the airport level. Additionally, TSA leadership contact information is on the website for program-related issues.

Question. How many complaints does TSA receive and what's the average time for complaints to be resolved?

Answer. At present, there is no single mechanism that captures all customer complaints, compliments, and inquiries. Currently, the system is not structured in a manner that separately breaks out numbers of compliments, complaints, and requests for information within any given subject matter category.

The TCC handles approximately 40,000 non-media inquiries or contacts from the traveling public, including complaints, on a monthly basis. In addition, TSA receives complaints, as well as other types of contacts, through other channels. For example, the Claims Management Office (CMO) receives approximately 2,400 claims on a monthly basis. Customer comments also come into TSA through Customer Support and Quality Improvement Managers at airports. At this time, there is no system that centrally tracks the complaints received by TSA through its various channels.

The time it takes to resolve any particular complaint varies depending on the nature of the complaint. In the majority of cases, the matter is resolved by the CSR or agent who initially handles the inquiry by providing the individual with information as to why a particular action was taken or about processes currently in place and the average talk time for these calls is approximately four minutes. The TCC does not currently track how long it takes to resolve a matter when an agent needs to elevate a call to a particular program office or the field for resolution.

Question. Is there a customer service function in TSA to take complaints at each airport and if so what types of training do these employees receive?

Answer. Many airports have a staff person assigned to manage the customer service function. The staff position is called Customer Support and Quality Improvement Manager (CSQIM). The CSQIM works closely with TCC to receive and respond to complaints and inquiries at the airport level.

Some airports have forms available for customer comments at the checkpoints. TSA headquarters is rolling out a pilot program at ten airports to test a standardized customer comment card. The card is designed to provide a means for convenient and quick feedback at the airport level.

Customer service courses are offered to CSQIM employees via the TSA online training center. Five customer service courses are now available (see descriptions below). An in-service training program, designed specifically for CSQIM employees, is being researched for future implementation.

Excellence in Service.—Fundamentals for Managers will help you develop the skills needed to effectively relate to customers, fulfill their basic needs, and exceed their expectations. You will be provided with opportunities to differentiate between internal and external customers, take ownership for customers' needs, and make sure your customers are completely satisfied.

In "Excellence in Service.—Working with Upset Customers," you will learn how to successfully serve upset customers, calm upset customers, and deal with abusive customers. In addition, you will learn how to control your own emotions and reduce your level of stress.

In "Excellence in Service.—Communicating with Your Customers," you will learn how to build rapport with your customers, and discover how non-verbal communication is interpreted by customers. In addition, you will learn telephone skills, including how to project professionalism and how to provide quality customer service over the telephone. Finally, you will learn how to communicate effectively with your customers through e-mail.

In "Excellence in Service.—Providing Superior Customer Service," you will learn how to develop and maintain a positive attitude, show extra attentiveness to your customers, and use customer-friendly language. In addition, you will learn how to effectively solve customers' problems and benefit from their complaints.

In "Excellence in Service.—Establishing Service Standards," you will learn what customers really want from your organization and how they evaluate your service, as well as how to create and implement effective service standards. In addition, you will learn how to monitor your service standards and how to correct problems that cause service to fall below the standards.

Question. Do you find that the complaints are related to TSA's security measures and the navigation through the airports or is it related to interactions with the airlines?

Answer. The TCC is responsible for handling all non-media inquiries from the traveling public. Each contact is assigned a subject category based upon the nature of the call. Among the available subject categories, one captures "Airline Issues" and another captures "Airport Issues." Airline issues generally involve matters related to proper identification, gate and boarding passes, baggage match and weight/size allowance, airline employee/service complaints, and refunds (airline tickets, lodging). Airport issues generally involve matters related to airport grounds, parking, checkpoint, configuration and limitations. Other categories capture a variety of TSA-related topics. In March 2005, the TCC handled 2,245 contacts involving airline issues, which represents approximately 5 percent of the total contacts handled. With respect to airport issues, 179 contacts were handled in March 2005, less than 1 percent of the total contacts. In addition to airline issues and airport issues, the TCC handled 9,106 contacts involving the No Fly list during March 2005.

R&D CONSOLIDATION

Question. The fiscal year 2006 budget proposes to consolidate all research and development of the Department of Homeland Security into Science and Technology, with the exception of the Domestic Nuclear Detection Office (DNDO). Mr. Secretary, can you tell us what the driving force is behind this consolidation?

Answer. Through the Homeland Security Act of 2002 and subsequent legislation, the Under Secretary for Science and Technology has been tasked with coordinating and integrating all research, development, demonstration, testing, and evaluation (RDT&E) activities of DHS and also to consolidate all Departmental research and development funding within the science and technology programs. The coordination and integration of RDT&E will: maximize the efficiency and effectiveness of the Department's RDT&E capacity; develop and expand synergistic RDT&E programs that cut across the Department's activities; create a world-class RDT&E capability; allow the other Directorates and organizational elements to eliminate within them the specialized management infrastructure required to manage organic RDT&E; and allow the other Directorates and organizational elements within DHS to focus on their operational missions.

Question. What savings do you hope to realize as a result of the consolidation?

Answer. This consolidation will bring under a single accountable authority the scientific and engineering personnel and other RDT&E resources of the Department. Coordination and integration of RDT&E will contribute to a synergistic environment wherein knowledge, capabilities, and initiatives can be leveraged and effectiveness and efficiencies can be enhanced.

Question. How will the consolidation change the way in which research and development is carried out within the Department today?

Answer. Consolidation will contribute to: maximize the efficiency and effectiveness of the Department's RDT&E capacity; develop and expand synergistic RDT&E programs that cut across the Department's activities; create a world-class RDT&E capability; allow the other Directorates and organizational elements to eliminate within them the specialized management infrastructure required to manage organic RDT&E; and allow the other Directorates and organizational elements within DHS to focus on their operational missions.

Question. What assurances can the Department provide to the Committee that the traditional mission of the Coast Guard will continue to flourish in the new consolidated research and development structure?

Answer. Authorities for the U.S. Coast Guard (USCG) RDT&E will rest within USCG, but the USCG RDT&E program will be coordinated with the overall departmental RDT&E program to maximize efficiency and minimize duplication of effort. There are significant efficiencies to be gained with an integrated RATE effort for the Department under a single accountable authority. The S&T Directorate is committed to and responsible for supporting the research, development, testing, and evaluation requirements to ehnance the USCG homeland and non-homeland security mission performance.

Question. Why isn't the DNDO research and development included in this consolidation, would it not benefit as well?

Answer. The Domestic Nuclear Detection Office (DNDO) serves as a unique entity within the Department to consolidate all nuclear-detection related activities, allowing for the development of an integrated office that will be responsible not only for research and development, but also for developing a global nuclear detection architecture and developing and implementing a domestic detection system, to include acquisition programs for detection assets and operational support functions. This integration, as well as coordination with nuclear detection programs in other departments, will allow for the development of a single, global nuclear detection architecture to protect the Nation from attempts to import or transport a nuclear device or fissile or radiological material intended for illicit use.

DNDO will continue to closely interface with the S&T Directorate on joint projects, as appropriate, for the development of technologies that may provide countermeasures against multiple threat types. The separation of the DNDO nuclear detection RDT&E from the RDT&E conducted within the S&T Directorate will be conducted so as to not have any detrimental effect on potential collaborative efforts that would be gained through the S&T consolidation effort. The goal is to make sure that this Nation maintains a preeminent research and development program to address the technical challenges in radiation detection science and technology, while at the same time capitalizing on the benefits of integrating this program with larger acquisition and operational support efforts.

DOMESTIC NUCLEAR DETECTION OFFICE

Question. Mr. Secretary, I understand from recent news reports that you established the Domestic Nuclear Detection Office 2 days after your arrival at the Department. Further, I understand this office was operational prior to your reorganization notification pursuant to the Homeland Security Act establishing this office directly under the Office of the Secretary. The Committee has also just received a reprogramming request to provide fiscal year 2005 resources to support this office. Where did you get the initial resources and staff to stand up this office?

Answer. The DNDO is a part of a natural evolution of the DHS S&T Radiological and Nuclear Countermeasures portfolio, which was appropriated $122.6 million in fiscal year 2005. Of this appropriation, $92.5 million was to be used to manage programs that directly fall within the mission space of the DNDO, as currently envisioned. The programs that currently are managed through this appropriation, along with the associated staff, will ultimately fall under the management of DNDO. Additionally, a number of other departments and DHS components have provided staff, on a non-reimbursable basis, to the DNDO transition team, which will eventually form the initial staff for the office.

The defense of this Nation against a terrorist nuclear attack is one of the top priorities of the Department, and the attention that I gave this matter immediately

upon my arrival should be indicative of that. I sent out a memo to the Department on March 16, outlining my intention to establish the DNDO, and directing senior members of the Department to support the transition and establishment of the office. This is a process that is still underway, rather than one that has been concluded. As part of this process, the Committee was notified, on April 13, of a single funding reprogramming to use existing DHS S&T funds, as appropriated, to cover operating costs of the new office for the remainder of fiscal year 2005. Simultaneously, I submitted, in accord with Sec. 872 of the Homeland Security Act of 2002 (Public Law 107–296), notification to Congress of the intent to establish the DNDO within the Department. On April 15, the President issued National Security Presidential Directive-43/Homeland Security Presidential Directive-14, "Domestic Nuclear Detection," directing the establishment of DNDO within the Department.

Question. The Department is required to come before the Committee and receive advance approval for new initiatives, why wasn't the Committee notified in advance of the Office's establishment?

Answer. On April 13, DHS submitted both an 872 notice and an fiscal year 2005 Reprogramming Report to appropriate Authorization and Appropriations Committee members. In anticipation of the notification to Congress, I previously announced to the Department my intent to create the office and established an acting director with authority to begin staffing the office from DHS and the other agencies involved, and to take necessary steps to be functional as soon as possible.

Question. Can you tell the Subcommittee what has changed in the last year to warrant the creation of this office immediately; is it new intelligence, new authorities granted to Homeland, or new vulnerabilities uncovered?

Answer. While there is currently no specific intelligence indicating when or where a nuclear attack might occur, it is expected to take several years to continue to develop and test effective, sustainable countermeasures and deploy and operate systems to interdict an attempted attack by our adversaries. With this in mind, it is important to take steps proactively to strengthen and consolidate efforts to be prepared if and when an attempt should come.

Accordingly, acting now provides the Department with an opportunity to consolidate all nuclear-detection related activities and proceed with a fully integrated approach that will include not only research and development, but also the development of a global nuclear detection architecture and development and implementation of a domestic detection system, including acquisition programs for detection assets and operational support functions. This integration, as well as coordination with nuclear detection programs in other departments, will allow for the development of a single, global nuclear detection architecture to protect the Nation from attempts to import or transport a nuclear device or fissile or radiological material intended for illicit use.

Question. The Department is taking great pains to consolidate the research and development of the Department under the Science and Technology Directorate. Would you explain the rationale behind why DNDO's research and development should remain separate?

Answer. The DNDO serves as a unique entity within the Department to consolidate all nuclear-detection related activities, allowing for the development of an integrated office that will be responsible not only for research and development, but also for developing a global nuclear detection architecture and developing and implementing a domestic detection system, to include acquisition programs for detection assets and operational support functions. This integration, as well as coordination with nuclear detection programs in other departments, will allow for the development of a single, global nuclear detection architecture to protect the Nation from attempts to import or transport a nuclear device or fissile or radiological material intended for illicit use.

DNDO will continue to closely interface with the S&T Directorate on joint projects, as appropriate, for the development of technologies that may provide countermeasures against multiple threat types. The separation of the DNDO RDT&E from the RDT&E conducted within the S&T Directorate will be conducted so as to not have any detrimental effect on potential collaborative efforts that would be gained through the S&T consolidation effort. The goal is to make sure that this Nation maintains a preeminent research and development program to address the technical challenges in radiation detection science and technology, while at the same time capitalizing on the benefits of integrating this program with larger acquisition and operational support efforts.

ROLE OF SCIENCE AND TECHNOLOGY DIRECTORATE

Question. As you step into the role of Secretary, Mr. Chertoff, how well do you think S&T is carrying out its strategic mission?

Answer. Over these last few months I have closely reviewed the work of the S&T Directorate and believe it is doing very well in carrying out its mission. The most important mission for the S&T Directorate is to develop and deploy cutting-edge technologies and new capabilities so that the dedicated men and women who serve to protect and secure our homeland can perform their jobs more effectively and efficiently. The S&T Directorate uses a risk-based approach to prioritizing and planning, and identifies critical capability gaps before attempting to identify or develop technology solutions. The S&T Directorate then addresses the highest priorities that address the broad threat spectrum as well as supporting the needs of the Department's organizational elements.

Question. During your short tenure, what are the areas of greatest concern to you?

Answer. As I emphasized in my recent 2SR speech, the Department's success in meeting its strategic objectives requires a coordinated risk-based approach to planning and prioritizing its activities, and this approach is being implemented across the Department. Thus, the development and implementation of effective and efficient counter-measures to biological, chemical and explosive threats continues to be an area of emphasis for the Department. Within the Department, the S&T Directorate has the lead in developing effective countermeasures for biological, chemical, radiological/nuclear, and explosives threat agents as well as providing support to the Department's organizational elements. The DNDO has the lead role in radiological/nuclear detection capabilities. Both the S&T Directorate and DNDO are committed to ensuring that the Nation is safer from these threat areas. Additionally, the S&T Directorate remains committed to providing the nation's emergency responders, Border Patrol, Coast Guard, and other members of the responder community with innovative, affordable technologies.

Question. How do we have any confidence that the Department, and S&T specifically, is heading in the right direction? Recent reports indicate that S&T has made little if any progress in actually increasing our security through research and strategic management of our limited research dollars.

Answer. Clearly, the S&T Directorate works to ensure that the nation's Federal, State and local operational end-users have the necessary technological tools to protect and secure our homeland. The S&T Directorate acknowledges and accepts that technology research and development is not a 6 month process but rather a long-term investment of 18 months to 4 years for the technology to mature. The Directorate tends to aim further down the road to ensure that the research and development being conducted today is capable of dealing with emerging threats in the future. All of the S&T Directorate's programs began at the same time, March 2003 or soon thereafter, therefore the S&T Directorate has not yet reached full maturity in many of its critical ongoing efforts.

The S&T Directorate also recognizes the need for technology solutions in the near term. The S&T Directorate's efforts to date have resulted in numerous products that are increasing our security. Included in these are:

—BioWatch, a biological agent detection system, which protects the nation's major population centers from the threat and ramifications of a bioterrorist attack. BioWatch also provided support during the G8, Democratic National Convention and Republican National Convention;

—Developed and transitioned PROTECT, a chemical detection system, to the Washington Metropolitan Area Transit Authority for use in the Washington subway system. PROTECT was also deployed to Boston and New York for the Democratic and Republican National Conventions and remains in the New York subway system;

—Delivered the Threat Vulnerability Integration System (TVIS) and the Threat-Vulnerability Mapper (TVM), to the Information Analysis and Infrastructure Protection (IAIP) Directorate;

—Developed the BTS Technology Vision which include Border Watch, Transportation Watch and Border Net which significantly improves our ability to provide the information necessary to secure our borders;

—Selected four urban areas for the pilot of the Regional Technology Integration (RTI) Initiative;

—Developed a joint port and coastal surveillance prototype designated HAWK-EYE with the United States Coast Guard; and

—Developed a Critical Infrastructure Protection (CIP) Decision Support System (DSS) focused on prioritizing investment, protection, mitigation, response, and recovery strategies related to Critical Infrastructure Protection.

Question. How is S&T assisting in the protection of our critical infrastructure and what relation does that have to the Department's efforts of the Information Analysis and Infrastructure Protection office?

Answer. The S&T Directorate supports the Information Analysis and Infrastructure Protection (IAIP) Directorate in the technical aspects of assessing threats to the nation's critical infrastructure. Through RDT&E, the S&T Directorate is providing specialized technical tools for intelligence analysis and knowledge synthesis. Analytical tools include software algorithms for data extraction, pattern discovery, semantic graph representation, visualization, and modeling and simulation. To support these tools, the S&T Directorate also provides tools to the IAIP Directorate, such as the Threat Vulnerability Integration System.

Terrorist capability assessments, which are being performed by the national laboratories, also provide expert scientific data and background information analyses to the IAIP Directorate. The specially developed tools greatly extend the capabilities of the commercially available analytical products that are used by the IAIP Directorate. They are designed to work on massive, multimodal, and distributed data sets and to provide real-time, higher accuracy visualization and modeling capabilities.

The S&T Directorate is also developing scientifically based, rational approaches for prioritizing critical infrastructure protection strategies, protection requirements, and resource allocations using modeling, simulation, and analyses to assess vulnerabilities, consequences, and risks; developing and evaluating protection, mitigation, response, and recovery strategies and technologies; and providing real-time support to decision makers during crises and emergencies.

There are several significant examples of this partnership.

For example, the S&T Directorate provides assistance to IAIP in evaluating the scientific and technical capabilities of terrorist groups and organizations to develop and deploy all WMD agents. This is an excellent example of a reciprocal supporting relationship, in that the IAIP Directorate needs S&T Directorate insight into technical issues, while the S&T Directorate needs IAIP Directorate insight into emerging threats. This "swap" of insight allows the S&T Directorate to meet its responsibility for the coordination of RDT&E needed to address those emergent threats.

In addition, countermeasures for WMD (such as chemical, biological, radiological and nuclear threats) are addressed within the S&T Directorate—however this work supports and is developed in coordination with all of the operational elements of DHS including the IAIP Directorate.

Furthermore, the S&T Directorate is developing the Critical Infrastructure Protection Decision Support System (CIP–DSS) in collaboration with several units of the IAIP Directorate and working with the IAIP Directorate's National Infrastructure Simulation and Analysis Center (NISAC) to validate and mature the model.

The S&T Directorate has also developed the annual National Critical Infrastructure Protection (NCIP) R&D Plan in close coordination with the IAIP Directorate. The National Infrastructure Protection Plan (NIPP), developed by the IAIP Directorate, and the NCIP R&D Plan are complementary documents, mutually supportive and coordinated.

Finally, the S&T Directorate, in coordination the IAIP Directorate, is leading RDT&E efforts that will improve the security of the existing cyber infrastructure and provide a foundation for a more secure infrastructure. To protect these infrastructures, we must improve the security of the protocols that underlie Internet communications. Technological advances are necessary to protect against, detect, and respond to attacks on the nation's information infrastructure.

The S&T Directorate has a number of cooperative programs with the IAIP Directorate linking cyber security research to critical infrastructure protection:

—*Process Control System Forum (PCSF).*—This forum was established to accelerate the development of technology that will enhance the security, safety and reliability of process control system (PCS) and supervisory control and data acquisition (SCADA) systems.

—*Control System Security Test Center (CSSTC).*—In collaboration with the Department of Energy and its resources and testing facilities, this program focuses on developing procedures for enumerating the vulnerability of process control systems to cyber attack and finding solutions to correct these weaknesses.

—*Small Business Innovative Research (SBIR) Awards.*—In fiscal year 2004, 13 Phase I SBIR projects were awarded in the area of process control system security. In fiscal year 2005, Phase II SBIRs were awarded to a subset of the Phase I performers, on the following topics: Advanced Security for SCADA Systems, Protection of SCADA Systems Using Physics Based Authentication and Location

Awareness, Improved Security Information Management for SCADA Systems, A Robust Secure Management System for SCADA/EMS Operations, and A Toolkit for Next Generation Electric Power SCADA Security Protection and Research.

The Science and Technology Requirements Council is one process by which the IAIP Directorate and the other component units in DHS convey their RDT&E requirements to the S&T Directorate. Representatives from the IAIP Directorate also are members of the S&T Directorate's Integrated Product Teams, a key mechanism for coordination and planning of DHS RDT&E efforts.

Question. What is on the horizon in terms of the newest threats and related countermeasures under development?

Answer. The Department is working in close collaboration with the DOD, the FBI, members of the Intelligence Community and others to identify potential new threats, assess the nations vulnerabilities to these potential new threats, and the consequences if these potential new threats were successfully used against us. The S&T has the responsibility within the Department to incorporate the risk of these potential new threats into our overall RDT&E process and the development of appropriate countermeasures. Although details can not be provided herein, the S&T Directorate is addressing, for example, potential threats from genetically modified biological organisms and certain types of non-traditional chemical warfare agents to develop appropriate countermeasures.

Question. Can you tell us how S&T has had a direct role in improving the security of the country?

Answer. The nation's advantage in science and technology is a key element in securing the homeland. The most important mission for the S&T Directorate is to develop and deploy cutting-edge technologies and new capabilities so that the dedicated men and women who serve to protect and secure our homeland can perform their jobs more effectively and efficiently. However, the threats to our homeland remain diverse and daunting. The S&T Directorate constantly monitors current and emerging threats and assesses our vulnerabilities to them, develops new and improved capabilities to counter them and mitigate the effects of terrorist attacks should they occur. The S&T Directorate also enhances the conventional missions of the Department to protect and provide assistance to civilians in response to natural disasters, law enforcement needs, and other activities such as maritime search and rescue. Basically the S&T Directorate assists in making DHS operations science-based, intelligence-informed and technology-enabled.

Question. Mr. Secretary, in the President's fiscal year 2006 request is $110 million for the counter man-portable air defense systems, or Counter MANPADS. Can you give us an update on the status of this program?

Answer. DHS is still on schedule to complete Phase II of the Counter MANPADS program and to provide its report to Congress and the Administration at the end of January 2006. This report will include a Concept of Operations, a maintenance approach, data on system effectiveness and reliability, options on how the system may be deployed, restrictions or regulatory changes required to comply with International Traffic in Arms Regulation (ITAR), and Life Cycle and Total Ownership cost estimates. BAE Systems and Northrop Grumman are scheduled to complete their system designs, including Critical Design Reviews in early summer of 2005. Following the review, the contractors will fabricate, install, and test their prototypes on commercial aircraft (late summer and fall of 2005).

By the end of January 2006, each contractor will have delivered two complete units and demonstrated system performance, including the results of studies emphasizing the operational suitability and cost of its systems. They also will have integrated their equipment onto aircraft, and obtained FAA Supplemental Type Certifications for aircraft airworthiness with the countermeasure system installed.

In addition, the requested $110 million provides for a Phase III program to improve operational, affordability, and maintainability issues. Based on interaction with airline stakeholders, an objective was established for system reliability that fits within the commercial airline heavy maintenance or major overhaul schedule of approximately 3,000 flight hours (depending on commercial airplane types).

A primary objective of the Phase III effort is to increase the reliability of the current countermeasure equipment by fielding a number of operational units and conducting laboratory reliability growth testing. DHS S&T estimates that the Phase III efforts will double current countermeasure equipment reliability to achieve the 3,000 hour threshold across airplane types. Additionally, operational and maintenance concepts have been developed, including reducing the requirements of Minimal Equipment List (MEL) and commercial supply chain management practices, that will be evaluated during Phase III. Based on the results of Phase III operational fielding, reliability testing, and evaluation of operational and maintenance procedures, system design alterations will be developed with ITAR considerations in

mind that will make fleet-wide fielding much more affordable and commercially viable.

Question. Are there areas within S&T where the strategic placement of dollars would be most efficiently used?

Answer. The S&T Directorate uses a risked-based approach to prioritizing and planning and identifies critical capability gaps before attempting to identify or develop technology solutions. The S&T Directorate then addresses the highest priorities across the broad threat spectrum as well as supporting the needs of the Department's organizational elements. The Directorate's R&D activities reflect the prioritization of efforts among the many possible threat agents and targets as well as technology development for supporting the organizational elements of the Department and the emergency responder community.

S&T UNIVERSITY PARTNERSHIP PROGRAM

Question. How does the University partnership effort improve DHS' ability to carry out its mission?

Answer. The Homeland Security Act of 2002, as amended, looks to the university community to stimulate, coordinate, leverage and utilize its unique intellectual capital to address current and future homeland security challenges. To maximize the benefits of engaging the multi-disciplinary research capacity of universities and to access current and future generations of researchers and practitioners, a number of focused activities have been established. These include multi-institutional Centers of Excellence built around mission-critical homeland security areas; cooperative research activities with other Federal agencies with homeland security responsibilities; support of undergraduate, graduate and postdoctoral students to develop a cadre of talent committed to homeland security programs; and outreach to the broader education community. These activities will help ensure that DHS will have the scientific knowledge and talent to successfully address homeland security challenges.

Question. Mr. Secretary, what unique role does S&T play with regard to university research and why is it important?

Answer. The S&T Directorate continues to identify knowledge and capability gap areas that need to be addressed to deal with current and future homeland security threats and the development of countermeasures to those threats. Many of these areas are well suited to university research, development and educational capabilities. Universities provide state-of-the-art research experts experienced and successful in cross- disciplinary programs, access to national and local talent pools and a neutral setting to consider important policy issues. These capabilities and ensuing cross fertilization directly benefit the operational responsibilities of the S&T Directorate.

Question. Are these projects that receive funding chosen by peer review and what does the Department gain by having funded a specific project?

Answer. All projects funded within University Programs are the result of a rigorous and competitive peer and relevancy review process. This includes all research and educational programs. With regard to the Centers of Excellence, in selecting research areas, the S&T Directorate seeks input from a variety of sources. These sources include the Homeland Security Act of 2002, as amended; the National Research Council (NRC); the Homeland Security Presidential Directives (HSPDs); other DHS directorates; and subject matter experts. DHS personnel interact extensively with the funded Centers of Excellence by serving on their review committees, attending workshops and exploring joint research initiatives. In this manner, DHS stays aware of their mission-critical research.

Question. Mr. Secretary, contained in the President's fiscal year 2006 budget request is $22.9 million for the National Bio and Agrodefense Facility. What is the mission of this facility and why isn't it in the Center for Disease Control's or U.S. Department of Agriculture's budget request?

Answer. HSPD–9 ("Defense of United States Agriculture and Food", paragraph 24) states: "The Secretaries of Agriculture and Homeland Security will develop a plan to provide safe, secure, and state-of-the-art agriculture bio-containment laboratories that research and develop diagnostic capabilities for foreign animal and zoonotic diseases." The S&T Directorate currently has responsibility for one such facility, as the Homeland Security Act of 2002 transferred the "assets and liabilities" of the Plum Island Animal Disease Center (PIADC) from USDA to DHS as of March 1, 2003. PIADC is currently the nation's only Bio-Safety Level 3 facility (BSL–3Ag) for research and diagnostic programs on foreign animal diseases such as foot-and-mouth disease (FMD). The bio-containment laboratories and animal facilities at PIADC are aged well beyond their originally designed life expectancy, and are in

immediate need of re-capitalization or replacement. There is no BSL–4 livestock capable laboratory at PIADC or elsewhere in the United States to work on high consequence zoonotic diseases in host livestock species. Therefore, planning for the National Biological and Agriculture Facility is the top S&T Directorate priority for biocontainment facilities, and impacts ongoing and planned programs for biological countermeasures for foreign animal diseases (including assays and diagnostics, vaccines and therapeutics, and forensics).

Recognizing the needs described above, the President requested $23 million in fiscal year 2006 for the design and initiation of a National Bio and Agro-defense Facility (NBAF). In preparation for this, we have undertaken a conceptual design study to better characterize the key programmatic requirements driving the NBAF design and to explore the cost benefit tradeoffs associated with each of these drivers. This conceptual design will explore three major NBAF options of increasing capability:

—Keeps the scope the same as the current PIADC mission but builds the facilities required to meet the needs of the first half of the 21st century;
—Expands the scope to include additional agriculture biocontainment laboratories for foreign animal and zoonotic diseases as called for in HSPD–9 above; and
—Adds expanded test and evaluation facilities to support clinical testing of medical countermeasures by the Department of Health and Human Services (HHS).
—DHS is committed to working with Congress, stakeholders, and partner Federal Departments and agencies (e.g. USDA and HHS) in the development of this new facility.

DHS INTELLIGENCE MISSION

Question. Mr. Secretary, your written testimony states that you will work closely with the intelligence community and the Director for National Intelligence. Given that, what is Information Analysis and Infrastructure Protection (IAIP) Directorate's role in the intelligence world since the enactment of the Intelligence Reform Act?

Answer. This role is evolving. The Department makes many contributions to the Intelligence Community and we will continue to enhance those contributions. Systematic intelligence lies at the heart of everything that the Department does. Understanding the enemy's intent and capabilities affects how we operate at our borders, how we assess risk in protecting infrastructure, how we discern the kind of threats for which we must be prepared to respond. We are enhancing our ability to fuse that information and combine it with information from other members of the Intelligence Community, as well as information from our State and local and international partners.

As I announced on July 13, 2005, I have proposed that the Assistant Secretary of Information Analysis become the Chief Intelligence Officer for the Department. My proposal is for the Chief Intelligence Officer to head a strengthened Intelligence and Analysis division that will report directly to me. This office will ensure that intelligence is effectively coordinated, fused and analyzed within the Department so that we have a common operational picture. It will also provide a primary connection between DHS and the Intelligence Community as a whole, and a primary source of information for state, local and private sector partners. The Department's unique access to information from our components, as well as our robust relationship with State, local, and tribal governments, as well as with the private sector, makes our enhanced contribution to the IC critical as we move forward.

In addition, since the creation of the Director of National Intelligence, IAIP, through the Office of Information Analysis, has collaborated with the Office of the Director of National Intelligence (ODNI) on a number of initiatives. IA works closely with the National Counterterrorism Center (NCTC). Among other things, we have provided IA intelligence analyst detailees to the NCTC, who are in a unique position to understand both intelligence information derived from our components and its impact on State and local governments, as well as the private sector. We also work closely with the NCTC to provide data and fuse critical information. We also participate in the WMD Working Group, (an outgrowth of the WMD Commission), the National Framework for Analytical Production working group, which is responsible for developing a national production framework for the IC, and on work dealing with human resource issues. IA will continue to develop a close working relationship with the ODNI as it strives to improve existing programs and put in place new initiatives that will further strengthen and protect our homeland.

Question. Is it the opinion of the Department that IAIP's functions are enhanced or minimized by the Act?

Answer. Greater integration of the Intelligence Community and a heightened emphasis on information sharing as a result of Public Law 108–458, the Intelligence

Reform and Terrorism Prevention Act of 2004 (IRTPA), will strengthen the ability of DHS's Office of Information Analysis to carry out its mission. We are optimistic that these reforms will lead to greater collaboration in analysis and greater ease of exchanging information across all levels. The continued emphasis on information sharing directed by IRTPA, for example, will improve DHS IA's ability to carry out its mission to fuse and lead the Department's intelligence activities and to share and receive critical threat information with and from state, local, territorial, and tribal governments and the private sector.

Question. Can you tell the Subcommittee how the Homeland Security Operations Center's (HSOC) daily activities are changed by the Intelligence Reform Act?

Answer. The daily activities of the HSOC are not changed by the Intelligence Reform Act. The HSOC will continue to provide general domestic situational awareness, a common operational picture, and support to the Interagency Incident Management Group (IIMG) and DHS Leadership, as well as act as the primary conduit for the White House Situation Room and IIMG for domestic situational awareness. HSOC collects domestic related suspicious activity reports throughout the United States and shares that information with DHS stakeholders.

Question. How will the HSOC perform its mission in light of this new Act?

Answer. HSOC will continue to perform its core missions as it has in the past.

Question. How has the Homeland Security Operations Center interfaced with the Terrorist Tracking Information Center which has been absorbed into the National Counterterroism Intelligence Center?

Answer. The HSOC provides general domestic situational awareness, a common operational picture, and support to the IIMG and DHS Leadership, as well as acting as the primary conduit for the White House Situation Room and IIMG for domestic situational awareness. The HSOC will continue to collect domestic related suspicious activity reports, look at domestic terror threats and natural disasters, focusing efforts domestically. HSOC is the lead conduit to State and local agencies. HSOC anticipates being the primary conduit to NCTC for domestic situational awareness.

Question. How will the Homeland Security Operations Center fit into the new intelligence community structure?

Answer. The advent of the new intelligence community structure does not significantly change the daily activities of the HSOC. The HSOC acts as the "ingest" point for threat traffic and suspicious activity reporting to DHS, so it is integral that the information captured and exploited by the Office of Information Analysis (IA) staff in the HSOC is shared with the Federal Intelligence Community. This occurs on a constant basis through video teleconference (0100 Production Meeting hosted by NCTC, the 0800 and 1500 SVTC), telephone, JWICS email and fax. The IA staff in the HSOC works closely with the NCTC Operations Center/FBI Counterterrorism Watch to develop emergent traffic containing a domestic nexus. Additionally, the IA staff in the HSOC is prepared to provide situational awareness to the DNI Operations Center when it is operational.

Question. Do you think the Department should have an Under Secretary of Intelligence to elevate its role within the intelligence community?

Answer. As I announced on July 12, 2005, after conducting 2SR, I believe that the current Assistant Secretary for Information Analysis should become the Chief Intelligence Officer for the Department, and that this component should report directly to me. I am confident that these changes will ensure an enhanced role for the Department's intelligence functions within the Intelligence Community.

CRITICAL INFRASTRUCTURE PROTECTION

Question. The Department recently released an interim report on the Nation's critical infrastructure, the purpose of which is to provide an outline for integrating critical infrastructure protection at the national level. How does this interim report lead to better protection of the Nation's critical infrastructure?

Answer. DHS is coordinating, for the first time, the overall national effort to protect critical infrastructure. The Interim National Infrastructure Protection Plan (NIPP) describes a risk management framework that takes into account threats, vulnerabilities, and consequences to prioritize the nation's critical infrastructure and key resources (CI/KR). The NIPP delineates roles and responsibilities among Federal agencies; state, local, and tribal entities; as well as private sector stakeholders in carrying out infrastructure protection activities within and across the 17 CI/KR sectors established by HSPD–7. The Interim NIPP is intended to foster sector-specific protective strategies and provides a mechanism for coordinating protective actions across sectors. It builds on the nation's existing critical infrastructure protection knowledge base while acknowledging the need to expand dialogue and

partnerships with key public and private sector stakeholders to create an integrated, national critical infrastructure protection program.

Question. My concern is that although the exercise is useful in developing a framework, when it gets down to the details, the momentum is lost and there never seems to be any achievements. How do you intend to use the interim report to translate into actual outcomes?

Answer. The interim NIPP outlines the foundation, processes, and methodologies of the risk management framework. The interim NIPP will be replaced by the final version of the NIPP, which will include sector-specific plans with performance measures.

Question. Did you seek the advice of States, locals and the private sector in the writing of this report?

Answer. Yes, as part of the comment period during July and August of 2004, the preliminary draft NIPP was shared with State and Territorial Homeland Security Advisors and individual members of the private sector for review and comment. The comments from the review were taken into consideration during the development of the Interim NIPP. The period of time dedicated to reviewing the Interim Plan will include additional private sector and stakeholder engagement.

Question. How does this report enable the Department to better identify which infrastructure is critical and what are the criteria for that determination?

Answer. The NIPP risk management framework sets over arching security goals. Once security goals are set, the next step in the framework is to develop and maintain an inventory of the nation's assets. After an asset is identified and basic information on it is collected, DHS employs an initial screening methodology to determine whether or not it is of national consequence. Priority is given to those assets that, if attacked, could have a nationally significant effect.

Question. How do you plan to get this report out to the public? Are you planning on doing town hall meetings, news articles or another forum?

Answer. The success of the national infrastructure protection program, as framed and articulated in the Interim NIPP, is highly dependent on obtaining buy-in and participation from all audiences. DHS is responsible for leading and coordinating the national infrastructure protection program, while the responsibility for carrying out the protective activities is shared among Sector-Specific Agencies, asset owners/operators, and state, local, and tribal governments.

State, local, and tribal entities and private sector stakeholders have an important role to play in protecting the nation's CI/KR. To ensure that assets within these areas are covered within the engagement and outreach process, these stakeholders must be aware of, and participate in, the implementation and the refinement of the Interim NIPP. The initial approach to engage state, local, and tribal entities and private sector stakeholders will be carried out by DHS, in coordination with the Sector Specific Agencies.

Stakeholder outreach and engagement tactics differ greatly by audience and focus on each stakeholder's interests and role in the implementation of a national infrastructure protection program. Accordingly, the Interim NIPP engagement process is organized by audience group, specifically: intra-Federal stakeholders; state, local, and tribal stakeholders; private sector stakeholders; and the media and public.

IAIP HIRING DIFFICULITIES

Question. Of concern to me is the amount of time it takes IAIP to hire and put in place new personnel. These are people who are charged with the intelligence and infrastructure protection functions of the Department. Why is it taking so long, and what can the Subcommittee do to help improve this situation?

Answer. As a result of the competitive market for the cleared community and the unique skills and abilities needed in IAIP, an aggressive recruitment of these talented candidates has been necessary to drive toward our hiring goals. As noted, these candidates are filling important intelligence and infrastructure protection functions. The process of recruiting, selecting, and hiring candidates to meet the Directorate's needs is lengthy because of the multiple steps involved in this process to ensure a complete and thorough evaluation of candidates. However, over the past year IAIP has been successful in implementing improvements to shorten this process.

Working closely with the Office of Personnel Management (OPM), improvements include the development of position descriptions and vacancy announcements that define the minimum requirements for each position. Once the position is posted and an applicant pool is created, a list of qualified candidates is then forwarded by OPM to hiring managers for comprehensive interviews and assessments. Once a selection

has been made, a tentative offer is extended to the candidate contingent upon the successful completion of a security investigation.

IAIP hiring managers take the time necessary in the selection process in order to ensure the specialized needs of the Directorate are met, particularly since many of the vacancies are highly sensitive positions.

Even faced with the competitive market for qualified candidates and the time it takes to on-board candidates, IAIP has been successful in hiring 517 of the 803 FTE allotments to date and will continue to aggressively recruit to meet its hiring target.

The Subcommittee has been very supportive in working with IAIP to understand the implications and expectations required to staff a highly qualified team. The approval to allow direct hiring authority has been instrumental in allowing us to aggressively identify, assess, and hire key staff. The continued active support of the Subcommittee is appreciated as IAIP works to achieve this target hiring goal.

Question. Is the hiring time dependent on another agency to process background checks and clearances?

Answer. Historically, DHS contracted collateral (SECRET and TOP SECRET) as well as TS/SCI security investigations through traditional venues such as Office of Personnel Management and Defense Security Systems (DSS). These venues also provide support to Federal, military and intelligence agencies. Due to high demand, they have continuously experienced severe backlogs, adversely impacting the timely processing of DHS requests.

However, DHS has recently acquired a new venue for security investigations through CBP. CBP now processes TS/SCI clearances for DHS and, due to a smaller workload, has cut down the average time for a security background investigation (with no previous clearance) from 12–18 months to as little as 6–8 weeks. This timeframe is competitive or, in many cases, faster than industry averages within the cleared community.

Under the current projected timeline of the hiring process, the security clearance process accounts for 25 percent of the total hiring process cycle time on average. This is a significant reduction from previous projections (50–60 percent), and is attributed to recent changes in the sourcing of investigations to a new contractor agency.

Question. Is the Department doing anything to help IAIP recruit qualified candidates for such a crucial role?

Answer. DHS has been fully supportive of IAIP recruitment efforts and has included the Directorate in a variety of Department-wide recruitment events to attract qualified candidates. For example, the Department was successful in obtaining direct-hire authority for IAIP's hard to fill positions and the Equal Opportunity Office has partnered with IAIP to attend a Disability Career Fair and Asian Pacific American Federal Career Advancement Summit. IAIP also participated in a DHS-wide career fair at Walter Reed Army Medical Center to recruit disabled veterans in conjunction with the Department of Defense, as well as a DHS-wide Presidential Management Fellows job fair at the Washington Convention Center during the last week in March of this year.

Question. Can you please submit your strategy to the Subcommittee on how you intend to address this problem?

Answer. IAIP is working to implement new ways to improve the candidate selection process to support surge hiring efforts. These include:

—*Posting All Remaining Vacancies.*—Work with hiring managers to expedite the posting of all vacancies on the USAJOBS website;

—*Making Multiple Selections.*—Encourage the practice of making multiple selections from Cert Lists whenever possible;

—*Sharing Cert Lists.*—Facilitate the sharing of Cert Lists are shared among managers with similar hiring needs;

—*Supporting the Recruitment Campaign.*—Encourage managers to attend recruitment events; and

—*Conducting Panel Interviewing.*—Identify Subject Matter Experts to screen qualified candidates for hiring manager review and selection.

Through these efforts, IAIP will institute a systematic process for identifying volume hiring needs, matching those needs with available candidates, and mobilizing hiring managers to make multiple selections in a timely manner. In support of this strategy, IAIP is continuing efforts to broaden the candidate pool through an active recruiting campaign targeting specific hiring needs and an aggressive advertising campaign to publicize opportunities at IAIP.

Question. Is the housing of IAIP personnel still an issue today?

Answer. Yes, housing remains an issue for IAIP, but we are working to overcome them. Among the challenges faced by IAIP is the lack of permanent space. On any given day, there are more than 90 IA employees without a dedicated seat. Staff have

been doubling, tripling, and quadrupling up in seats, working shifts and staggered hours to compensate for the deficit of Sensitive Compartmented Information Facility (SCIF) seating.

To address its facilities situation, IAIP has developed a plan through fiscal year 2006 to place staff in swing and permanent seats on the NAC, and five floors of leased space at an office building in Arlington, VA. The Arlington location is currently partially occupied as swing space while floors are permanently constructed in a planned series. Two floors are nearing completion of permanent construction, with furniture and IT installation to follow. The entire project is scheduled for completion at the end of 2005. The location will eventually have 440 seats, and will house primarily the Office of Infrastructure Protection (IP).

On the NAC, IAIP will occupy part of Building, all of Building 19, and the first and second floors of Building 17. Ultimately, all of Building 19 will be SCIF and will house IA (to include seating for the positions requested in 2006) and the Office of the Under Secretary. Floors one and two of Building 19 are under demolition/power upgrade prior to renovation, which is currently scheduled to be completed in Winter of 2005, with the renovation beginning in the Summer of 2005 and continuing into the Spring of 2006.

IAIP's total SCIF requirement will be met once the Building 19 renovation is completed.

IAIP COORDINATION OF PROTECTION

Question. How does the Department plan to get the necessary support of State and local governments and private sector to protect our critical infrastructure when dollars are tight?

Answer. DHS relies on strong and cooperative relationships with State and local governments and private sector partners to advance overall National protective strategies. The Department understands that local law enforcement, first responders, and the overall readiness and response community have the day-to-day responsibility to protect our citizens and infrastructures. The Federal Government must continue to partner with State and local officials and key leaders in the private sector to ensure available funding is appropriately allocated and correct policies and procedures are in place.

The Department will continue to cultivate and expand its outreach and information sharing components to enhance its relationships with state/local and private sector partners. By continuing to build upon these vital relationships, the Department plans to continually provide the information, policy guidance and risk assessment methodologies necessary to help owners and operators bolster physical and cyber security plans.

Question. How does the Department coordinate with all other efforts by the Federal Government and State and locals, including municipalities to ensure that each entity is putting in place the most effective security measures for a specific piece of infrastructure?

Answer. As part of an ongoing, government-wide effort to protect national infrastructure, DHS is working on several initiatives with other Federal departments, state, local, and tribal governments, and the private sector. These initiatives are designed to protect against known and potential threats; reduce critical infrastructure vulnerabilities in a comprehensive and integrated manner; maximize efficient use of resources for infrastructure protection; build partnerships among Federal, state, local, tribal, private sector, and international stakeholders; and continuously track and improve national infrastructure protection.

In the first of these initiatives, the Department is providing the private sector, law enforcement entities, and State homeland security personnel with technical and material assistance to develop and implement Buffer Zone Protection Plans (BZPPs) around critical infrastructure and key assets. To formulate these plans, owners and operators and local law enforcement work together to identify asset vulnerabilities, gaps in protection, and means of mitigating these vulnerabilities.

The Department is also in the process of deploying all 68 Protective Security Advisors (PSAs) to 60 metropolitan areas throughout the United States. These security specialists serve as DHS representatives permanently assigned in the field. The mission of the PSA is to represent the Office of Infrastructure Protection (IP) in local communities throughout the United States, serving as a liaison between DHS, the private sector, and Federal, state, local, and tribal entities; acting as IP's on-site critical infrastructure and vulnerability assessment specialist; providing expertise and support to the Principal Federal Official(s) responsible for National Special Security Events; and providing real-time information on facility significance and

protective measures. PSAs continue to assist local entities in putting in place the most effective security measures for specific pieces of infrastructure.

DHS is also providing terrorism prevention training to private sector, law enforcement entities, and State homeland security personnel. To date, over 5,600 security personnel have participated in the training courses. Courses relate terrorist threats and tactics to one of several different topics including buffer zone protection plans, soft targets, bombs, underwater hazardous devices, police S.W.A.T. team response, and counter surveillance and emerging threats. This training program provides baseline knowledge for a law enforcement protecting critical infrastructure.

Finally, Government Coordinating Councils (GCCs) are groups being established for each sector that consist of Federal representation involved in the security of all 17 sectors defined by the National Infrastructure Protection Plan (NIPP). The GCCs will serve as a counterpart to industry-sponsored Sector Coordinating Councils (SCC). GCCs, which include a number of agencies with sector infrastructure protection responsibilities, will coordinate with the SCC and work to ensure the implementation of effective sector strategies and initiatives to support the nation's homeland security mission.

Question. What are IAIP and the Department doing about cybersecurity, particularly when it is not governed by any one actor but affects everyone?

Answer. The National Cyber Security Division (NCSD) of IAIP's Office of Infrastructure Protection was created to address cyber security issues and the priorities laid out in the National Strategy to Secure Cyberspace. In addition, HSPD–7 called upon the Department to establish a national focal point for cyber security, which is the mission of NCSD. Both the National Strategy to Secure Cyberspace and HSPD–7 recognize that cyber security is not just one entity's concern or jurisdiction, and both call upon DHS to be a focal point and work with partners in other Federal agencies, academic institutions, the law enforcement and intelligence communities, the private sector, and the general public to improve our cyber security posture.

NCSD's mission, in cooperation with public, private, and international entities, is to secure cyberspace and America's cyber assets. In order to fulfill that mission, NCSD has laid out goals that reflect and guide its priorities and programs, as follow:

—*Goal 1.*—Establish a National Cyber Security Response System to prevent, predict, detect, respond to, and reconstitute rapidly after cyber incidents.

—*Goal 2.*—Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks.

—*Goal 3.*—Promote a comprehensive national awareness program empowering all Americans to secure cyberspace.

—*Goal 4.*—Foster adequate training and education programs to support the nation's cyber security needs.

—*Goal 5.*—Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace.

In addition to the National Strategy to Secure Cyberspace, Homeland Security Presidential Directives, National Security Presidential Directives, the Federal Information Security Management Act (FISMA) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets; recognizes the highly networked nature of the current Federal computing environment and provides effective government wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities; provides for development and maintenance of minimum controls required to protect Federal information and information systems; provides a mechanism for improved oversight of Federal agency information security programs; acknowledges that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the Nation that are designed, built, and operated by the private sector; and recognizes that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products. Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center US–CERT to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

FISMA, Section 3546 states that the Federal information security incident center, US–CERT, will perform the following functions:

—Provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;
—Compile and analyze information about incidents that threaten information security;
—Inform operators of agency information systems about current and potential information security threats and vulnerabilities; and
—Consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters. In accordance with DOD Directive O–8530–1, all DOD services and agencies are to report incidents to the Joint Task Force Global Network Operations (JTF–GNO), which will, in turn, coordinate directly with the US–CERT.

The DHS approach to cybersecurity is one of coordination and collaboration. Therefore, in each of its cybersecurity efforts, DHS works with key stakeholders and subject matter experts, both within the Department and with external constituencies on a Federal, State, local, and international level.

OFFICE OF SECURITY

Question. What is the Department doing to streamline the process of security clearances to prevent a backlog?

Answer. The Department grants access to classified information in a timely manner. There is no adjudicative backlog in the granting of security clearances at the present time.

The Department is continually working to improve the process of conducting and adjudicating background investigations and granting security clearances. DHS is coordinating with other departments and agencies in the personnel security community to accomplish this goal.

Reciprocity.—DHS, like other Executive Branch Departments and agencies, complies with the requirements of Executive Order 12968, which establishes a uniform Federal personnel security program for employees who require access to classified information. The Intelligence Reform and Terrorism Prevention Act and Executive Order 12968 require that background investigations and eligibility determinations should be mutually and reciprocally accepted by Federal agencies. Since its inception, DHS has conformed to this reciprocity requirement.

Interim Secret Security Clearances.—The Department grants interim access to certain classified information following favorable completion of a preliminary investigation. This interim Secret clearance permits DHS employees to begin their service expeditiously. In addition, the Department is working diligently with the Office of Personnel Management to accelerate the investigative process for Top Secret security clearances by obtaining delegations of authority and prioritizing cases.

Certain Investigative Authority.—DHS has obtained certain investigative authority that expedites background investigations and re-investigations for Top Secret and Sensitive Compartmented Information (SCI) security clearances. The Department has utilized the personnel security services of CBP in the Border and Transportation Security Directorate to conduct these background investigations for DHS Headquarters applicants. In this way, DHS has been able to avail itself of process improvements, technological advances, and other management efficiencies.

Additional Adjudicators.—The DHS Office of Security (OS) is hiring additional Federal employees as security clearance adjudicators to meet the Department's growing needs.

Streamlining the Process.—In addition, DHS has taken the following steps to streamline and improve the quality of the security clearance process:
—The Department is focusing its background investigations on the areas most relevant to the current threats facing the country and the Department;
—The Department is applying resources in the early phases of the investigation to maximize limited investigative resources and minimize wasteful expenditure on candidates unlikely to be favorably adjudicated;
—The Department is strategically placing employees to assist other Federal agencies at key points of the investigative process;
—The Department is automating many aspects of the personnel security process, including the deployment of Electronic Questionnaires for Investigations Processing (EQIP), an automated tool that allows applicants to complete the form online, thus reducing the processing time and minimizing the error rate; and

—A team of human capital and personnel security experts are working to increase efficiency by educating managers and prospective employees about the requirements of the security clearance process.

Question. A pending fiscal year 2005 reprogramming request proposes to transfer $6.6 million from the Information Analysis and Infrastructure Protection Directorate to the Office of Security. Will the fiscal year 2006 request of $39.4 million for the Office of Security fully fund the Office of Security so that it does not require transfers from other DHS components to carryout its important operations?

Answer. It is projected that the increase of $39.445 million for fiscal year 2006 will be sufficient for the currently-anticipated requirements of the Office of Security. It should be noted, however, that the proposed House version of the fiscal year 2006 Homeland Security Appropriations Bill cut of $10 million would have a drastic effect on important operations. If this occurs, the Office of Security will again require a transfer of funds from other components or be forced to cut services.

Question. How will the Office of Security assist with the Department's efforts to improve information sharing with State and local governments and private industry?

Answer. The Office of Security (OS) aims to facilitate the sharing process, while ensuring that the dissemination of information is conducted through secure processes and channels to trustworthy individuals. OS continues to play an integral role in the Department's efforts to improve information sharing at all levels through a number of initiatives.

OS has assisted in the following ways:

—*Security Clearances.*—OS has established and implemented processes to facilitate the issuance of security clearances to state, local and private sector personnel, in coordination with the SLGCP and the Infrastructure Coordination Division of the IAIP Directorate.

—*Communications Security.*—OS has developed standards and a process for the deployment of secure communications equipment, in coordination with SLGCP and the DHS Chief Information Officer;

—*Computer Security Standards.*—OS has developed and implemented standards that support the deployment of computer equipment for classified information disseminated to selected State and local government locations;

—*Security Policy Guidance.*—OS has issued policy and procedural guidance to support the sharing of information and encourage secure dissemination to the intended audience; and

—*Security Training.*—OS has prepared and distributed educational and awareness products to designated State and local government personnel and private-sector officials.

OS has played a significant role in the creation of proposed national standards for the sharing and safeguarding of homeland security information.

Question. What coordination will take place between the Office of Security, the Chief Information Officer, and the Information Analysis and Infrastructure Protection Directorate to ensure that sensitive security materials do not fall into the wrong hands?

Answer. The Office of Security (OS) continues to coordinate with the DHS Chief Information Officer (CIO) and the IAIP Directorate to ensure that information shared with state, local and private sector partners is afforded the appropriate protections commensurate with the level of sensitivity.

In addition to the five areas listed in the previous response, OS has: (1) contributed to the development of policies and procedures for the deployment of the HSDN and is an active participant in the Homeland Security Accreditation Working Group, developing guidelines regarding appropriate physical security standards, security clearance verifications, and security training for the HSDN program; (2) provided guidance regarding the "Need to Know" requirements for the network. In addition, OS has contributed to the creation of a Homeland Security Information Network-Secret (HSIN–S) Users Manual to ensure proper security standards for information disseminated through the system; (3) involved in a comprehensive review of information sharing laws, Executive Orders, regulations and guidance, and it has participated in the creation of national standards for the protection of sensitive and classified homeland security information; and (4) participated in weekly meetings with the IAIP Information Sharing and Collaboration Office, a program established to coordinate and facilitate information sharing throughout DHS and with its partners.

REGIONS INITIATIVE

Question. Why has the report required by section 706 of the Homeland Security Act of 2002 not been submitted to Congress?

Answer. The report required by section 706 of the Homeland Security Act of 2002 was submitted in February 2004 as requested.

Question. The fiscal year 2006 budget justification proposes a traveling cadre from the Office of Security that will provide security-related support to regional offices. However, there is no funding identified for this activity. How will the Office of Security provide assistance to these offices without funding?

Answer. The Office of Security is requesting a total of $168,131 for travel in the line item fiscal year 2006 budget. This money will be used by Office of Security personnel to support all travel requirements within the office.

I-STAFF

Question. The Operational Integration Staff and the proposed Office of Policy, Planning, and International Affairs appear to be working toward the same goal of developing cohesiveness among DHS components. How are the roles of the integration staff distinguished from those of the proposed Office of Policy, Planning, and International Affairs?

Answer. The new Office of Policy will lead the Department in both strategic policy development and oversight of all program policy efforts, while consolidating programs with significant policy responsibilities into one cohesive office. The new Office of Operations will provide the Department with a coordinated cross-cutting operation function. The Operation Integration Staff, consequently, will no longer be needed, and most of its current employees will be merged into the Offices of Policy or Operations

Question. The Department has placed the Operational Integration Staff in charge of coordinating the security plans for homeland security events that are not designated National Special Security Events (NSSEs). Please provide an overview of the plan for operational command and control for such events?

Answer. Special Event security is the responsibility of law enforcement agencies with jurisdiction at the event location. The lead agency will normally be the local law enforcement agency. However, a Federal agency may assume the lead role, as with an event at a national park. Generally, because multiple agencies and jurisdictions are involved, a coordinated and integrated approach to event security is involved. As directed by both the Homeland Security Act of 2002 and HSPD–5—"Management of Domestic Incidents," the Department of Homeland Security promulgated the National Incident Management System (NIMS). The NIMS provides a command and control framework within which government and private entities at all levels can work together across each phase of incident management: prevention, preparedness, response, recovery, and mitigation. Specifically, the NIMS requires the formation of a Unified Command to facilitate coordination for incidents and potential incidents involving multiple agencies with independent jurisdictional authority. The Unified Command allows agencies with different legal and functional authorities and responsibilities to work together in an integrated fashion without affecting individual agency authority, responsibility, or accountability. For Special Events below the NSSE threshold, the responsibility for security planning resides entirely within this Unified Command.

The NIMS also recognizes the need for support and coordination for an event and establishes a multi-agency coordination system comprised of local and State Emergency Operations Centers and coordination entities. Under normal circumstances, there is no similar standing Federal coordination entity at the local level, but certain special events below the NSSE threshold create a significant need for Federal interagency coordination. In such cases, the Secretary of Homeland Security appoints a Federal Coordinator to serve as the principal Federal point of coordination. As requests for Federal assistance are answered and as Federal agencies adapt their independent authorities, the Federal Coordinator captures this integrated strategy in the form of a Special Event Integrated Federal Support Plan. The Federal Coordinator then coordinates support and information sharing at the special event and responds to unforeseen support needs and events.

The NIMS protocol does not change the existing command and control architecture at the Unified Command level for agencies supporting the Unified Command, or for agencies forced to adapt their independent operations as a result of an event.

Question. What role (if any) will the Secret Service have in non-NSSE events?

Answer. For non-NSSE events, i.e., DHS-established levels of Special Events Homeland Security (SEHS), the role of the Secret Service will vary dependent upon the circumstances surrounding the particular event. For events that receive a designation of Level I or Level II and have a traditional protectee of the Secret Service in attendance, the Secret Service will implement appropriate protective protocols and may serve as the Federal Coordinator. For events that receive a designation of

Level I or II that do not have a traditional Secret Service protectee in attendance, the Secret Service may offer available protective assets, as appropriate.

When the event receives a lower designation and a protectee will attend, the Secret Service will implement appropriate protective protocols; in those instances when no protectee will attend, the Secret Service may offer protective event management training, as appropriate.

Question. What is the budget for the Operational Integration Staff for fiscal year 2005? Where are those funds coming from?

Answer. As directed by the language in the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief Act, 2005, further funding is not available for the Operational Integration Staff in fiscal year 2005 unless funds are reprogrammed. Travel and incidental costs were borne by the components of those on detail to these efforts.

HUMAN RESOURCES

Question. In developing a human resources system that is mission-centered and performance-focused, how will the creation of open pay ranges and performance pay pools assist the Department in meeting its operational needs?

Answer. A major objective of open pay ranges is to provide DHS management with the flexibility to compete with other employers (private, Federal, State and local), and to attract, hire, and retain the best candidates for positions within the Department. DHS management will have increased flexibility in negotiating employee salaries. Under a pay-for-performance system, the objective is to truly compensate those employees who have made significant contributions to accomplishing the agency's mission. Employees will play a major role in determining their eligibility for performance adjustments based upon their work performance. The intent is to motivate employees to perform their very best; as a result, this incentive should assist significantly in enhancing agency effectiveness and employee retention.

Question. A total of $53 million is included for Max HR in the fiscal year 2006 budget request. What is the total projected cost of the Max HR system?

Answer. The total anticipated cost for the period fiscal year 2005–2008 is $250 million. This amount is broken down as follows:

The total funding includes $43 million for training 100,000 employees, which is essential to ensure that the new HR flexibilities achieve the desired results. This funding will train all Department executives, managers, supervisors, and employees on all aspects of the new system and their responsibilities as leaders in the DHS environment, and to provide the framework for all of the components to work together as one Department of Homeland Security. Comprehensive training also will be provided for HR professionals throughout DHS whose roles and responsibilities are impacted by implementation of the new HR provisions.

Additionally, $56 million in funding will be used for detailed systems design and implementation support and to provide access to experts who are assisting in designing the new DHS performance management system, job evaluation system (including the creation of job clusters), compensation system (including new pay ranges and market pay processes), and linkages for pay and performance. This in-depth expertise is required to ensure DHS creates a program that appropriately links pay, competencies, performance, and labor market, and through this linkage, improves DHS' mission performance and accountability.

$100 million will be required to fund the initial conversion of over 90,000 employees from the General Schedule pay system to newly created market-based pay ranges. This amount will cover one-time conversion costs for employees included in three implementation phases. Phase 1 of the DHS pay conversion, which is scheduled for January 2006, covers employees in DHS HQTRS, S&T, IAIP, OS, U/S MGMT, U/S BTS, FLETC, and EP&R, and is estimated to cost $10 million. Phase 2, which will occur in January 2007, will include U.S. Secret Service and U.S. Coast Guard (civilians). Phase 3, the largest phase covering CIS, CBP, and ICE, will occur in fiscal year 2008.

A total of $9 million is required to fund the new Homeland Security Labor Relations Board (HSLRB) in fiscal year 2005 and 2006. The Board has been established in fiscal year 2005 as an independent entity that will report to the Office of the Secretary. The HSLRB resolves labor-management disputes and is integral to the deployment of the labor relations section of the regulations. $42 million for program management funding is required for program evaluation and to manage appropriate cost, schedule, and control activities at the Departmental level, ensuring that the system investment is managed appropriately and at a good value. Program management funding will provide for earned value management assessments and risk man-

agement. This funding will also ensure the development of a robust metrics and program management evaluation framework that will be used to gauge overall program success. In addition, department-wide communications about MAXHR will be funded from the program management account.

Question. The budget request for fiscal year 2006 includes $10 million to fund the initial conversion of some Homeland Security employees from the General Schedule to newly created market-based pay ranges. Does the Department expect any delays in this conversion to the new system?

Answer. We expect to be on schedule in converting to the new system. DHS employees will be converted to the new pay system in three phases. Phase 1 occurs in January 2006; Phase 2 occurs in January 2007 and Phase 3 occurs in January 2008.

NAC

Question. The budget request provides $26.1 million to continue expansion of the Department's presence at the Nebraska Avenue Complex. What is the Department's estimated timeline for standing up a fully operational Nebraska Avenue Complex?

Answer. We expect to be 70 percent to 80 percent occupied at the NAC within 6 to 9 months of the U.S. Navy vacating the site based on minor renovations to the site as planned and barring any significant infrastructure changes as found during earlier moves within the NAC. The U.S. Navy is expected to vacate the site by December 31, 2005, so we would expect to be 70 percent to 80 percent occupied between May 2006 and August 2006.

We expect to be 100 percent occupied at the NAC within 18 to 24 months (May 2007-October 2007) of the U.S. Navy vacating the site based on the planned major renovations of several buildings at the NAC.

Question. Is there a timeline for the United States Navy to be completely relocated to another facility?

Answer. Yes, December 31, 2005.

Question. Are there projected cost estimates on what the Department will be required to pay for relocation of Navy activities?

Answer. Yes, the original U.S. Navy relocation cost estimates were established between GSA, U.S. Navy, and DHS with OMB review. DHS' share to relocate the U.S. Navy was estimated to be approximately $30,800,000. Of this amount, $12,500,000 was obligated for this purpose in fiscal year 2003 and fiscal year 2004. DHS obligated $12,000,000 year to date in fiscal year 2005 and expects to obligate the remaining $6,300,000 in fiscal year 2005 for a total obligation of 18,300,000 in fiscal year 2005.

FINANCIAL AND PROCUREMENT CONTROLS

Question. What is included in the fiscal year 2006 budget request to improve the CFO's oversight and controls of the Department's bureaus?

Answer. The Office of the Chief Financial Officer (OCFO) fiscal year 2006 budget request includes substantial increases that will enable OCFO to increase its level of oversight and control of the DHS components. OCFO has requested two additional FTEs and $305,000 to increase budget execution oversight of the components. Whereas OCFO conducted mid-year budget execution reviews of the components in fiscal year 2005, the additional staff will allow us to conduct quarterly reviews in fiscal year 2006 and beyond. More staff in the OCFO budget division will allow a redistribution of desk officer portfolios; reduced portfolio sizes will allow all OCFO budget desk officers to work more closely with component budget personnel and to intensify oversight of the components' budget execution. This will allow for more timely identification and resolution of problems in components that require additional oversight. One additional FTE and $152,000 will augment the OCFO's appropriations liaison staff and ensure timelier fulfillment of the appropriations committees' requests.

The request for OCFO also includes five additional FTE and $763,000, and $4,000,000 for technical assistance to implement the DHS Financial Accountability Act. In order to implement the Act, the DHS OCFO will design and implement DHS-wide policy, procedures, and internal controls. The goals of the Act imply that DHS must accelerate consolidation of financial operations. Additional FTE and funding will enable the OCFO to increase financial policy guidance and for OCFO financial analysts and contractors to work closely with the components' financial operations on internal control and standardization projects. Increased interaction will lead to more consistent and better financial performance at DHS.

Question. The budget request proposes funding of $9 million, an increase of $1 million, for the Chief Procurement Officer. As the majority of the funds for this of-

fice have been proposed through the Working Capital Fund, are there sufficient funds for the Procurement Office in the fiscal year 2006 budget request?

Answer. Yes, the fiscal year 2006 increase of $1 million for the Office of the Chief Procurement Officer (OCPO) is sufficient. The OCPO provides acquisition policy, oversight, strategic sourcing, competitive sourcing, integrated systems, and grants policy support for the entire Department. The Office of Procurement Operations, a direct report to the OCPO, is funded separately through the working capital fund and provides operational contracting support to 35 major organizational components including S&T, IAIP, the Offices of the Secretary and Deputy Secretary, and the Under Secretary for Management.

Question. The Department's organizational structure places the Chief Procurement Officer under the Office of the Under Secretary for Management, while other offices like the Chief Financial Officer are funded separately. Would altering this structure to make the Chief Procurement Officer a direct report to the Secretary of Homeland Security help to improve this office's ability to provide oversight to all Department procurements?

Answer. To ensure the administrative functions of the Department are properly integrated, the OCPO should continue to report directly to the Under Secretary of Management and the OCPO's budget should remain a part of the USM budget. Changing the OCPO's reporting structure and/or segregating the OCPO's budget would have no material impact on the Department's ability to provide oversight of the procurement program.

DEEPWATER

Question. Mr. Secretary, the Coast Guard has submitted to Congress a revised baseline of its Deepwater acquisition plan. How confident are you that the Coast Guard has accurately reestimated the use of its assets in this post 9/11 environment?

Answer. The original Deepwater System contracted in 2002 was based on the Coast Guard's 1998 mission demand. I am confident that the revised Deepwater implementation plan reflects the changed requirements of the Deepwater system needed in the post-September 11 environment.

We revised the Deepwater implementation plan based on a comprehensive performance gap analysis that identified new capabilities that the Coast Guard needed to carry out its responsibilities under the DHS Strategic Plan. The original, pre-September 11 Deepwater Program was then modified to incorporate these improved post-September 11 capabilities. The revised plan includes retaining, upgrading, and converting aviation legacy assets as part of the final asset mix and adjusting the program's overall asset delivery schedule to align with operational priorities. The revised plan also includes those capabilities necessary to provide maritime domain awareness and operate successfully in the post-September 11 threat environment. To help ensure the new plan meets broader national and departmental maritime homeland security and interoperability requirements, my staff carefully reviewed and analyzed the revised baseline prior to its approval by the DHS Investment Review Board (IRB). The Department's Joint Requirements Council and IRB also reviewed and approved the plan. The level of analysis and critical thinking that is reflected in the revised Deepwater plan exceeds that of any project that the Department has ever undertaken. For these reasons, I am confident that it will deliver the post-September 11 capabilities needed.

Question. Do you believe there will be further revisions to this plan? If so, why?

Answer. The revised implementation plan provides us with the right mix of assets to ensure its readiness to address current threats. However, the implementation schedule and the planned acquisitions will necessarily adapt to changes in annual appropriation levels and changes in other variables, such as technology upgrades and legacy asset conditions. The revised capabilities and capacities presented within the revised implementation plan are the result of nearly 2 years of analysis, gap assessment, and third party validation after September 11, 2001.

Question. A review of the fiscal year 2003 through fiscal year 2006 budgets indicates that the percent of Deepwater funds spent to sustain legacy ships, aircraft and communications systems climbed each year from 7 percent in the fiscal year 2003 budget to 25 percent in the fiscal year 2006 budget. This is very troubling given that the objective of the program is to reduce the cost of maintaining legacy assets within the Deepwater system. What can be done to reverse this trend and bring new ships and aircraft into the fleet sooner?

Answer. Full support of the President's fiscal year 2006 Deepwater budget request is critical to ensuring urgent legacy asset projects, such as HH–65 re-engining, are funded to immediately correct existing deficiencies while providing significant re-

capitalization funding for procurement of assets to replace those that are rapidly declining.

The Department is taking steps to mitigate legacy asset costs through advancing recapitalization of certain asset classes within the Deepwater program. For example, the fiscal year 2006 Deepwater request includes $108 million to advance acquisition of the Offshore Patrol Cutter by completing the design and purchase of long lead materials for the first cutter. The revised Deepwater plan also advances the acquisition of the Fast Response Cutter.

In addressing legacy asset maintenance issues, the Department has to balance four factors: operational needs, legacy fleet status, current Deepwater acquisition priorities, and available funds. Through sound resource planning and performance assessments we will invest the necessary resources to sustain operational assets until they can be replaced/recapitalized through the Deepwater project.

Question. Is it true that the Coast Guard's major cutters and much of your aircraft fleet are simply beyond their reasonable service life?

Answer. Many Coast Guard legacy assets are aging, technologically obsolete, and require replacement and modernization. The majority of these assets will reach the end of their planned service life by 2010. Coast Guard cutters and aircraft are failing at an alarming rate. However, with proper maintenance and sustainment support, the Coast Guard plans to sustain legacy assets at a level that will allow them to capably perform their missions until they are replaced by their Deepwater counterparts.

The President's fiscal year 2006 Budget requests $966 million for the Deepwater program, which includes critical funding necessary to address immediate legacy asset sustainment issues that threaten the performance of Coast Guard missions, including HH–65 re-engining and the Medium Endurance Cutter Mission Effectiveness Project (MEP). Full support of the President's Budget is critical to sustaining Coast Guard operational performance.

Question. Two years ago, at Congress' request, the Department provided an assessment of the feasibility of accelerating the Deepwater program. At the proposed fiscal year 2006 funding level of $966 million can we expect to accelerate the program?

Answer. The President's fiscal year 2006 Deepwater budget request of $966 million represents a 33 percent increase over the fiscal year 2005 enacted funding level of $724 million. It advances the delivery of the Fast Response Cutter by 10 years and the Offshore Patrol Cutter by 5 years, while beginning the conversion of legacy assets to meet post-September 11 mission requirements. Because of the additional capabilities and revised asset mix included in the revised Deepwater implementation plan, the total program is planned for completion completed in 25 years.

Question. What funding level would be required in fiscal year 2006 and future years to complete the plan within 10 years?

Answer. The President's Budget and the Department support the revised Deepwater implementation plan and the funding stream that acquires it in 25 years at $24 billion. To complete the plan within the next 10 years would require an annual funding stream between $1.7 billion to $2.2 billion per year.

Question. What, if any, improvements in operational effectiveness do you expect once Deepwater is fully implemented?

Answer. The post-September 11 Deepwater system will significantly enhance the Coast Guard's operational effectiveness. The initial Deepwater implementation plan was designed to meet the Coast Guard's missions in 1998. The post-September 11 asset capabilities included in the revised Deepwater implementation plan not only ensure the Coast Guard can meet its new maritime homeland security missions, but also enhance the Coast Guard's ability to meet its traditional mission requirements. Specific operational enhancements contained in the revised Deepwater plan include:

—Improved maritime security capabilities on selected Deepwater cutters, including greater speed, larger flight deck, and automated weapons systems to reduce maritime risk and enhance response to terrorist threats;

—Network-centric command, control, computer, intelligence, surveillance, and reconnaissance (C4ISR) systems to improve maritime domain awareness and interoperability;

—Helicopter airborne use of force and vertical insertion capabilities to provide warning and or disabling fire at sea and in ports, waterways, and coastal regions and to enable the delivery of boarding teams to board and take control of non-compliant vessels;

—Improved long-range surveillance capability to support maritime domain awareness and reduce the maritime patrol aircraft flight hour gap;

—Enhanced all-weather self-defense capabilities on select assets; and

—Improved Chemical, Biological, Radiological, and Nuclear/Explosive threat response on select Deepwater assets.

HH–65 HELICOPTER RE-ENGINING

Question. What is the status of the HH–65 re-engining project? Be specific in terms of how many engines have been replaced.

Answer. In August 2004, the first re-engined HH–65 was delivered to the Coast Guard at Aviation Training Center Mobile, AL, for operational testing and evaluation. As of the September 1, 2005, 10 re-engined HH–65Cs had been delivered for full operational status to Air Station Atlantic City, NJ, (5), Aviation Training Center Mobile, AL, (1), and Air Station Savannah, GA, (4). To accelerate the HH–65 re-engining project the Coast Guard and its contractor, Integrated Coast Guard Systems (ICGS), have examined the quality and suitability of a second re-engining facility located in Columbus, MS. In August 2005, this facility delivered its first re-engined aircraft to the Coast Guard. This aircraft was determined to meet needed quality and suitability parameters and the Coast Guard contracted with ICGS to re-engine an additional 11 aircraft at the Columbus facility. The Coast Guard plans to have all 84 operational aircraft re-engined in early 2007.

Question. Can all the engines be recapitalized within the specified timeframe given the current capacity at Elizabeth City, NC?

Answer. Given the current capacity at Elizabeth City, NC, the re-engining project cannot be completed within the specified timeframe. In order to complete re-engining the operational fleet of 84 helicopters by February 2007, the Coast Guard's Deepwater contractor, Integrated Coast Guard Systems, will rely upon a second re-engining facility at Columbus, MS.

Question. What will have to be done by the Coast Guard to meet the Congressional direction to re-engine the entire fleet within that required 24 month time period?

Answer. Provided the President's request of $133.1 million for HH–65 re-engining in the fiscal year 2006 budget is fully funded, the Coast Guard plans to complete re-engining of the operational fleet of 84 aircraft by February 2007. This is the fastest possible timeline based on the availability of engine kits and parts, increased production at the Coast Guard's Aviation Repair and Supply Center, and additional production capacity at a second facility. ICGS is assessing the quality and suitability of a second facility in Columbus, MS. That facility is now re-engining a single aircraft that is scheduled to be completed in September 2005.

Question. Will a second line be required?

Answer. In order to finish re-engining as quickly as possible and to meet the February 2007 timeline, a second line will be required.

Question. What lessons have been learned from the test helicopter currently being re-engined at the second line which the subcontractor has established at its site?

Answer. It is too early in the process to assess lessons learned. To accelerate the HH–65 re-engining project, the Coast Guard and its contractor, ICGS, are examining the quality and suitability of a second re-engining facility located in Columbus, MS. This facility is expected to deliver its first re-engined aircraft to the Coast Guard in September, 2005. Before making a final determination on the suitability of the facility the Coast Guard is evaluating the second facility's capabilities to control cost, meet schedule requirements, and employ standardized industrial processes.

Question. What value do you see in having a second line outside the Coast Guard's depot-level maintenance facility?

Answer. Using a second production facility will allow completion of the re-engining of all 84 operational HH–65s by February 2007.

Question. What are the challenges of a second line?

Answer. The second facility has not yet been certified as providing a quality product at a reasonable price. Also, as in any lead asset production, there is a substantial learning curve. Other challenges include:

—Validation of capability;
—Cost control;
—Avoidance of schedule delays;
—Parts availability; and
—Standardized industrial process.

COAST GUARD/C–130

Question. In the past, the Defense Appropriations Subcommittee funded the acquisition of 6 new C130Js, which are the next generation beyond the C–130Hs, and began funding to missionize these planes in fiscal year 2005. The President's budget

proposes missionization costs to be borne by the Coast Guard in fiscal year 2006. The cost of these planes has been outside the original Deepwater plan, but now the associated missionization costs are included in the revised Deepwater plan.

What legacy sustainment issues are you experiencing with the C–130H fleet?

Answer. On April 20, 2005, the Coast Guard submitted a legacy asset report to Congress, as directed in the Conference Report accompanying the fiscal year 2005 DHS Appropriations Bill. This report includes the HC–130H AC&I projects that the Coast Guard has included in the fiscal year 2006 budget request and anticipates requesting in future budget submissions. The primary HC–130H sustainment issues are as follows:

APS 137 Surface Search Radar ($75M, cost reflects conversion on 27 aircraft). The Coast Guard's fiscal year 2005 Deepwater budget includes $9 million to start the replacement effort for the HC–130H's APS 137 search radar

Avionics Modernization and Rewiring ($144M, cost reflects 16 aircraft). The HC–130H requires a modernized and supportable cockpit. This cockpit modernization will prepare the aircraft for the inevitable U.S. Airspace restrictions due to increased traffic and the Open Skies policy of route traffic control. Logistically, the aircraft's current cockpit instrumentation will become unsupportable within this decade. With plans for the HC–130H to operate until 2033, this will be a necessary upgrade. Over 500 other DOD aircraft are conducting the same modification. DOD modernization plans will significantly reduce the availability and or support of older parts, resulting in increased repair costs of the existing system.

Center Wing Box Structural Issues. In March 2005, the C–130 manufacturer, Lockheed Martin Aero (LMA), changed the inspection guidelines for C–130 wing boxes based on cracking found in Air Force C–130s of about the same age as some of the Coast Guard HC–130Hs. The wing box problem is not unique to the Coast Guard, but applies to all C–130's world wide. As a result of flight hour limitations and or restrictions identified in LMA Service Bulletin (SB1), the five Coast Guard 1500 series airframes are limited to restricted operations until they are properly inspected over the next 6 months. A second service bulletin is due this month from LMA that will provide the inspection criteria. The estimated cost of completing the 1500 series inspections is $2 million total. The remaining 22 aircraft are newer and will be due for inspections over the next 2 years.

Question. Now that the missionization of the Coast Guard's C–130 fleet is included in the Deepwater plan, what are the future costs to complete this undertaking?

Answer. The Coast Guard plans to have all six C–130J aircraft missionized and available for maritime patrol aircraft work by the end of 2008 at a cost not to exceed $120 million. Funds to complete this missionization were previously provided outside of Deepwater. Additional missionization costs within Deepwater are not currently anticipated. The President's fiscal year 2006 Budget request also includes $5 million to fund the Aircraft Project Office, which manages the C–130J pilot and air crew training, logistics use, and missionization oversight while the aircraft are transitioning to full operational use. As indicated in the fiscal year 2006–2010 Capital Investment Plan (page 116 of the Coast Guard's fiscal year 2006 Congressional Justifications), this cost will recur at $5 million per year through project completion in fiscal year 2008.

Question. Why were these costs omitted in the original Deepwater plan?

Answer. The Congressional Conference Report (H. Rept. 106–710) of June 2000 stated "That the procurement of maritime patrol aircraft (C–130J funded under this heading) shall not, in any way, influence the procurement strategy, program requirements, or down-select decision pertaining to the Coast Guard's Deepwater Capability Replacement Project." Based on this direction the Coast Guard did not include the C–130J in the original Deepwater plan.

Question. Since the acquisition and initial missionization costs of the C–130Js were incurred by the Department of Defense, do you believe that any future costs should also be borne by that Department?

Answer. Department of Defense funding already received in past years is sufficient to complete missionization of the C–130J aircraft. The President's 2006 budget includes a request for $5 million for the Coast Guard to fund the Coast Guard Aircraft Project Office, which will manage the C–130J pilot and crew training, logistics use, and missionization oversight while the aircraft are transitioning to full operational use.

Question. Why shouldn't the Department of Defense continue to complete this effort?

Answer. Funding to acquire and fully missionize the Coast Guard's six C–130J aircraft has already been provided through Department of Defense appropriations. The remaining funds required to complete the project, as outlined on page 116 of

the Coast Guard's fiscal year 2006 Congressional Justifications, should be borne by DHS appropriations since they will be used to train Coast Guard C–130J pilots and crews, fund Coast Guard logistics support, and transition the aircraft to operational use for Coast Guard missions.

RESEARCH AND DEVELOPMENT

Question. Has the Coast Guard R&D program been able to successfully support the Coast Guard's traditional mission areas since the Coast Guard is now an entity under the Department of Homeland Security?

Answer. Yes, the Coast Guard Research and Development program has been able to continue research in non-homeland security (traditional) mission areas. Presently, the Coast Guard is concentrating much of the traditional mission R&D effort on aquatic nuisance species remediation. The Coast Guard is also continuing research and development in other non-homeland security mission areas such as Aids to Navigation, Search and Rescue, Maritime Safety, and Marine Environmental Protection.

Question. How successful has the Coast Guard R&D program been in competing for DHS Science and Technology funding in addition to its own R&D budget?

Answer. The Coast Guard has been successful in competing for DHS S&T funding for homeland security-related projects. In accordance with established S&T protocols, the Coast Guard Portfolio Manager at S&T submits the Coast Guard Maritime Security requirements to the DHS S&T Executive Review Team for evaluation and funding. To date, the Coast Guard has received over $6.5 million of funding from the S&T Directorate in fiscal year 2005.

Question. Do you have any concerns about having this program transferred to the Science and Technology Directorate?

Answer. No, a collaborative relationship between the Coast Guard and the S&T Directorate is both viable and valuable. Integration of funding and research requirements will maximize the effectiveness of both homeland and non-homeland security research.

Question. How can you ensure those Members with concerns about traditional mission research that the Science and Technology Directorate (S&T) will place the same level of consideration on those areas of research as the Coast Guard does?

Answer. Retaining the Coast Guard's capabilities in both homeland and non-homeland security mission areas is of critical importance to DHS. Equally important is the retention of the Coast Guard's research and development capability in both homeland and non-homeland security (traditional) missions. The S&T Directorate is committed to and responsible for supporting the research, development, testing, and evaluation requirements for the entire Department, which includes enhancing the Coast Guard's homeland and non-homeland security mission performance. For example, to date the S&T Directorate has provided $7.56 million toward Project Hawkeye, an initiative that will enhance performance across the entire spectrum of Coast Guard missions by improving Maritime Domain Awareness.

Question. If Coast Guard R&D is transferred into S&T, what role does the Department plan for the Coast Guard Research and Development Center in Connecticut to continue to play in the future?

Answer. The Coast Guard R&D Center is the sole Government entity performing research and development in the area of Aids to Navigation, Search and Rescue, Maritime Safety, and Marine Environmental Protection. The Coast Guard R&D Center will continue to be the critical link to ensure the Coast Guard has the essential research, development, testing, and evaluation requirements to succeed in both its homeland and non-homeland security mission areas.

Question. What follow-on actions is the Coast Guard taking in response to the Congressionally-mandated study of Coast Guard R&D?

Answer. The Coast Guard is taking several of the study's recommendations for action. Key items include: the development and implementation of an overarching Research and Development strategy; continued outreach to other government agencies, industry and academia to establish partnerships; and improved alignment with the Coast Guard Acquisition Program.

COMMUNICATIONS AND TECHNOLOGY SYSTEMS

Question. Why has Rescue 21 been delayed so significantly? The GAO has been very critical of the Coast Guard's acquisition management team known as Deepwater. Isn't this just another example of the Coast Guard not being able to manage large acquisitions?

Answer. Rescue 21's delay in achieving initial operating capability (IOC) is due to problems experienced by General Dynamics C4 System (GDC4S). Those problems

have been twofold in: (a) completing software development needed to integrate the multiple commercial items into a consolidated control interface and (b) resolving performance issues stemming from System Integration Testing (SIT). Software integration and SIT issues have been resolved and the project is ready to enter full rate production upon approval.

The Coast Guard does not consider this delay a result of mismanagement as it has closely followed Coast Guard and DHS acquisition processes, as highlighted by the GAO Report 03–1111 Coast Guard's Rescue 21 Faces Challenges. GAO noted that the Coast Guard has developed key documentation used for managing system requirements and that the Coast Guard has a system in place for identifying, prioritizing, and minimizing risks.

The Coast Guard has successfully managed and executed several comparable acquisitions in the past. Recent projects such as Seagoing Buoy Tenders ($618 million), Coastal Patrol Boats ($327 million), and the Great Lakes Icebreaker ($140 million) were each remarkably successful. The Coast Guard will continue to seek out process improvements and apply past lessons learned to manage the Rescue 21 acquisition.

Question. Please provide an update on achieving full operating capability. What capabilities will Rescue 21 have at the end of fiscal year 2006?

Answer. Provided Rescue 21 is funded consistent with the Coast Guard's Capital Investment Plan outlined on page 116 of the Coast Guard's fiscal year 2006 Congressional Budget Justification, the Coast Guard expects Rescue 21 to reach full operating capability in fiscal year 2007. At the end of fiscal year 2006, deployment of Rescue 21 to all continental U.S. coastal regions will be complete.

Question. When will Rescue 21 transition to replace the National Response Distress System (NRDS), which is being supplanted by Rescue 21?

Answer. The Rescue 21 system will be deployed incrementally in all Coast Guard Sector/Group Regions. Following deployment and testing within each Coast Guard Sector/Group Region, the legacy NDRS in the affected region, will be removed and the Rescue 21 system will become operational. Nationwide deployment is expected to be complete in fiscal year 2007.

Question. When is NRDS expected to come offline?

Answer. The Rescue 21 system will be deployed incrementally in all Coast Guard Sector/Group Regions. Following deployment and testing within each Coast Guard Sector/Group Region, the legacy NDRS, in the affected region, will be removed and the Rescue 21 system will become operational. Nationwide deployment is expected to be complete in fiscal year 2007.

Question. Please provide an update of your planned Vessel Tracking System installation recapitalization schedule. When will the project be completed?

Answer. The Ports and Waterways Safety System (PAWSS) installation/recapitalization has been completed in five ports with two additional ports to be completed in the fourth quarter of fiscal year 2005, pending completion of remote site leases. Project closeout and transition of all systems to long-term operations and support will occur by the end of fiscal year 2006. Automatic Identification System (AIS) capability, which is an integral part of PAWSS, has been installed in all nine scheduled Vessel Traffic Service (VTS) ports.

Question. How will funding interruptions affect the project schedule, for instance, if funding is not provided in fiscal year 2006 what will not get done?

Answer. VTS systems in Puget Sound and San Francisco will not be recapitalized with funding provided to date. The Coast Guard's fiscal year 2006 Unfunded Priorities List includes $17 million for the PAWSS, the funding required to complete VTS recapitalization in these ports.

Question. Please provide an update on the progress/status of implementation of the nationwide Automated Identification System (AIS), especially as it relates to the maintenance of the Coast Guard's common operating picture.

Answer. The Nationwide AIS project has been approved and chartered by the DHS. The project is in the requirements and planning phase of the acquisition process.

Concurrently, numerous initiatives are underway to provide prototype and interim AIS capability to provide AIS data to the National Maritime Common Operational Picture (COP). The progress to date includes:

—Installation of AIS capability at all Vessel Traffic Services (9 sites).

—Deployment of receive-only AIS sites in key locations in Alaska (8 of 11 AIS sites).

—Deployment of 4 prototype AIS receivers on National Oceanic Atmospheric Administration weather buoys to provide AIS tracking of vessels offshore of the United States.

—AIS receiver installations for research & development purposes:

—On Oahu that provides extensive coverage of the major Hawaiian Islands;
—In San Francisco Bay, CA;
—In Miami, Port Everglades and Key West, FL; and
—In Long Island Sound, Cape May NJ, and the Cape Cod Canal.
—Installation of AIS sites on offshore platforms in the Gulf of Mexico to monitor traffic inbound to Gulf ports (3 of 4 planned AIS sites installed).
—Deployment of AIS receiver as part of a concept validation on a low earth orbit satellite for long-range AIS vessel tracking to be launched in the second and third quarter fiscal year 2006.

Question. How does AIS implementation fit with Ports and Waterways Safety System (PAWSS) and Rescue 21?

Answer. The Coast Guard, thru the PAWSS project, has deployed AIS capability in all nine VTS areas. Rescue 21 replaces the Coast Guard's antiquated short range command and control communications systems and it does not include AIS. The Nationwide AIS project will share infrastructure with Rescue 21 wherever site and technical compatibility will allow, e.g., towers.

Question. How is it different from PAWSS?

Answer. The AIS is a cooperative vessel tracking system whereby vessels transmit their position, identification, speed, course, cargo, and other information to vessels in their area and shoreside receivers within range of the system. The Maritime Transportation Security Act of 2002 specifies AIS carriage requirements for certain vessels navigating U.S. waters. The Nationwide AIS project will implement necessary infrastructure to receive AIS transmissions from shipboard systems and distribute this data to the Coast Guard's Common Operational Picture to enhance maritime domain awareness.

The PAWSS project was established to build new Coast Guard Vessel Traffic Service (VTS) systems and to modernize and recapitalize existing ones. The Coast Guard operates VTS in nine U.S. ports to provide traffic information, traffic organization, and navigation assistance services necessary to fulfill the Coast Guard's statutory maritime safety and environmental protection responsibilities under the Ports and Waterways Safety Act of 1972. PAWSS/VTS employ AIS, among other surveillance systems to monitor and access information on vessel movements within a VTS area.

A table highlighting the basic tenants of each project is provided below:

Compare/Contrast	Nationwide AIS	PAWSS
ACRONYM	Automatic Identification System	Ports and Waterways Safety System
Primary User	U.S. Coast Guard, Commercial vessels.	U.S. Coast Guard, Commercial vessels
Focus	Pre-9/11—Safety: for ship to ship to communicate rules of the road. Post-9/11—Safety and Security—Maritime Domain Awareness (MDA).	Pre-9/11—Safety Post-9/11—Safety and Security (Maritime Domain Awareness)
Purpose	Track vessels approaching, entering, and transiting U.S. navigable waters.	Manage vessel traffic in nine U.S. ports
Project	Enhance the nation's maritime domain awareness, safety, and security.	Provide Vessel Traffic Service
Line of Sight Transmissions	Send and receive: Data, ship-to-ship, ship-to-shore, shore-to-ship.	Send and Receive (& share): Voice & Data, AIS-based; radar & cameras
Location	Ports, waterways and coastal areas out to 2000 nautical miles via towers, buoys, offshore platforms, e.g., oil rigs, & satellite(s).	9 U.S. ports: one each in AK, NY, MI, CA, WA; two each in LA and TX

Question. Is PAWSS still needed or is it being phased out?

Answer. The PAWSS, as an acquisition project, is being phased out. The Coast Guard established PAWSS as an acquisition project to build new Coast Guard VTS and modernize existing systems. The PAWSS project resulted in two new VTS's, recapitalized five of the existing VTS's completely, and partially modernized two others (Puget Sound, WA and San Francisco, CA).

While there will be no more acquisitions completed through the PAWSS project, the Coast Guard VTS will still operate, providing navigation services and ensuring safety and environmental protection of U.S. waters as required by the Ports and Waterways Safety Act of 1972.

Question. How is AIS different from Rescue 21?

Answer. The AIS is a cooperative vessel tracking system whereby vessels transmit their position, identification, speed, course, cargo, and other information to vessels in their area and shoreside receivers within range of the system. The Maritime Transportation Security Act of 2002 specifies AIS carriage requirements for certain vessels navigating U.S. waters. The Nationwide AIS project will implement necessary infrastructure to receive AIS transmissions from shipboard systems and distribute this data to the Coast Guard's Common Operational Picture to enhance maritime domain awareness.

The Rescue 21 project will replace the existing and obsolete National Distress and Response System (the system used by the boating public to hail the Coast Guard when in distress) and provide the Coast Guard with a modern coastal command, control, and communications system. Rescue 21 will be capable of monitoring the international VHF–FM distress frequency to improve search and rescue response operations and communications with Coast Guard and other Federal, state, and local first responders and commercial recreational boats.

A table highlighting the basic tenants of each project is provided below:

Compare/Contrast	Nationwide AIS	Rescue 21
ACRONYM	Automatic Identification System	Formerly: National Distress and Response System (NDRS)
Primary User	U.S. Coast Guard, Commercial vessels.	U.S. Coast Guard, commercial, boating public
Focus	Pre-9/11—Safety: for ship to ship to communicate rules of the road. Post-9/11—Safety and Security—Maritime Domain Awareness (MDA).	Pre-9/11—Primary—Safety Secondary—support all other CG/DHS missions post-9/11—same
Purpose	Track vessels approaching, entering, and transiting U.S. navigable waters.	Command, control, and communication system to allow USCG to hear and locate mariners in distress
Project	Enhance the nation's maritime domain awareness, safety, and security.	Modernize the USCG's legacy NDRS
Line of Sight Transmissions	Send & receive: Data, ship-to-ship, ship-to-shore, shore-to-ship.	Send and receive: Voice and Data
Location	Ports, waterways and coastal areas out to 2000 nautical miles via towers, buoys, offshore platforms, e.g., oil rigs, & satellite(s).	Towers and vessels in 46 regions throughout the United States, including Guam and Puerto Rico

FEDERAL LAW ENFORCEMENT TRAINING CENTER (FLETC)

Question. Mr. Secretary, as you complete your top to bottom review of the Department, what emphasis will you place on the need to provide basic and advanced training to law enforcement personnel at the Federal Law Enforcement Training Center?

Answer. Standardized, high quality training is an exceptionally critical component in the success of the DHS responsibilities. The Federal Law Enforcement Training Center (FLETC) is the government's principal provider of interagency law enforcement training and is DHS's primary source for intradepartmental law enforcement training. FLETC already has accelerated the number and types of training programs being offered in concert with its Partner Organizations since the September 11, 2001, terrorist attacks. While basic training continues to be the first scheduling priority for FLETC, there has been a greater emphasis placed upon relevant advanced training to meet the post-September 11 focus on security of the homeland. FLETC has undertaken an initiative for Counterterrorism and Practical Applications Training, which provides hands-on experience for trainees at all levels to handle first responder situations, prevention and appropriate follow-up investigative

measures. Further, FLETC has a major role in international, State and local training with an emphasis on strengthening coordination with Federal law enforcement entities, to include intelligence sharing training. Under DHS's auspices, the Department anticipates relying heavily upon the enhanced and innovative training and increased physical plant capacities now available at the four FLETC sites in Charleston, SC; Cheltenham, MD; Artesia, NM and Glynco, GA.

Question. Do you anticipate opportunities for cross-training of law enforcement personnel?

Answer. One of the principal reasons for the creation of DHS is to continuously improve the overall cooperation, coordination information sharing and interoperability of law enforcement components at all levels related to security for the United States. To help bring about this improvement, DHS is encouraging greater measures that are intended to breakdown traditional organizational and cultural barriers. Cross-training and shared training experiences of multiple agencies is becoming more the norm. FLETC's approach to consolidated training, which emphasizes common understanding and cooperation through mixed class association, affords agencies the opportunity to benefit from mutual experiences. Many of FLETC's basic and virtually all of its advanced programs are scheduled to accommodate multiple training organizations. In the area of counterterrorism training, subjects such as weapons of mass destruction, critical infrastructure, crisis management and land and seaport security are open to all agencies with those needs. These include DHS, Department of Justice, Department of Defense and many others across the spectrum of law enforcement. DHS expects to expand and enhance training that is relevant and contemporary to the evolving needs of all agencies that are involved with the homeland security.

Question. Mr. Secretary, will your assessment examine the various training facilities owned or used by Departmental entities to ensure that they are being fully utilized and not duplicative of each other?

Answer. Training facilities, per se, were not themselves a specific focus of the review. Training has several different elements in DHS, from the general training of our employees, to our law enforcement academy, and to our training centers for first responders. Our plan brings together DHS' key preparedness programs, including first responder training programs. The U.S. Fire Administration and the Noble Training Center are moved into a new Preparedness Directorate, along with the training programs such as those at Ft. McClellan. The purpose for creating this Directorate, and for pulling these programs together, is to give our existing preparedness efforts—including training and exercises—a focused direction. With these programs in one Directorate, DHS will be in a better position to ensure that they are being fully utilized without being duplicative.

Question. Mr. Secretary, the war on terror requires a new approach to training law enforcement personnel. Do you foresee the need to provide new types of training infrastructure or counterterrorism training facilities that mirror our existing vulnerabilities?

Answer. Yes, the future operating environment of DHS will include continuing and increasingly sophisticated terrorist threats to our nation. Post-September 11, the FLETC, the primary law enforcement training organization for the DHS, began vigorously reviewing its training programs and developing and/or revising programs and facilities as appropriate to better prepare agents and officers in executing their duties in the Global War on Terrorism. The FLETC developed a plan and is currently in the planning design and execution construction phase for this type of infrastructure. The practical application counterterrorism training facility design is based on the FLETC and its Partner Organizations expertise on anti/counterterrorism operations and related training requirements to defeat terrorism. The FLETC offers the most current law enforcement training curricula available anywhere and has the instructional experience and expertise to meet the challenges set forth by our adversaries. However, to accentuate our training and meet these challenges, we continually upgrade our tactical facilities and construct training facilities that are responsive to the stated needs of the agencies engaged in the war on terrorism. The FLETC trains officers and agents from 81 Partner Organizations. It is imperative that we attempt to replicate the types of environments that our officers will surely encounter, to enhance their probability of survival and the success of guarding our homeland.

Consolidated training, the concept on which the FLETC was established, allows agencies with divergent missions to train together, in a consistent manner. This proposed training facility will meet the Department's primary goals to prevent terrorist attacks, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. This initiative represents the proactive "imagination," cited in the 9/11 Commission's report, needed to combat terrorism effectively.

The FLETC and DHS have been called upon by the Military to provide up-to-date Counterterrorism training. As the Military's mission changes, they have been expected to perform more like a Law Enforcement Officer rather than a soldier. The urban environments and circumstances that our soldiers face replicate the Use of Force decisions that our police officers face everyday. This mission change has forced the necessity for greater interaction between Law Enforcement and the Military. The FLETC has and continues to be a willing partner in meeting these challenges.

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

AVIATION SECURITY

Question. The Department's inspector general released a report yesterday stating that there has been a lack of improvement over the last year in detecting dangerous items—including guns, knives, explosives—at airport security checkpoints. What role will next generation detection systems play in improving airport security?

Answer. TSA has designed its passenger checkpoint technology portfolio to incorporate solutions that will help improve explosives and weapons detection at its checkpoints. The next generation of checkpoint technology will automate the detection of explosives that might be concealed on an individual's body, as well as within the carry-on baggage/items they are carrying. Additionally, TSA is exploring body imaging technologies that will allow screeners to detect weapons (metallic and nonmetallic) and explosives that an individual might attempt to hide on their person.

Question. Pilot programs at our airports play a critical role in moving technology from the research stage to practical deployment. What is the status of pilot programs for aviation security checkpoint detection technology, and when will these pilot programs begin?

Answer. TSA has initiated a number of operational testing and evaluation pilot projects involving the next generation of checkpoint technologies to expand TSA's explosives detection capabilities. Highlights from ongoing pilot programs are as follows:

Explosive Trace Portals (ETP).—TSA has deployed 15 ETPs to 14 airports nationwide to evaluate their operational efficiency and effectiveness for screening passengers for explosives. These pilots have been initiated at the following airports and are scheduled to continue through summer 2005: Rochester, NY; JFK, NY; Gulfport, MS; Baltimore, MD; Jacksonville, FL; Phoenix, AZ ; Miami, FL; Providence, RI; Las Vegas, NV (2 units); Los Angeles, CA; San Francisco, CA; Boston, MA; Tampa, FL; and San Diego, CA. TSA has allocated $28.3 million for the purchase and installation of additional trace portals in fiscal year 2005.

Explosive Trace Detection Document Scanners.—TSA is operationally testing and evaluating an explosives detection document scanner at 4 airports: Ronald Reagan Washington National (DCA), Los Angeles International (LAX), John F. Kennedy International (JFK), and Chicago O'Hare International (ORD). The current technology requires that the screener manually handle the travel document to obtain the sample needed for analysis to determine if traces of explosives are present. Based on the preliminary results of the pilot at the four airports, TSA has determined that an automated solution better suits operational and security needs. Consequently, the project has been refocused to develop a technology solution that will meet those needs. A pilot project for the automated prototype will be scheduled as soon as that product is determined ready for an operational test and evaluation.

Question. There is a critical need to identify new and emerging technology, in addition to explosive detection systems, to provide enhanced security protections at our nation's airports. Could you tell us what other progress the Transportation Security Administration (TSA) has made in identifying appropriate technology to improve the security and efficiency of the current airport passenger screening process?

Answer. In addition to the operational test and evaluation pilots underway using explosives detection trace portals and explosives detection document scanners, TSA has a number of R&D projects underway to expand both weapons and explosives detection capabilities. These projects include, but are not limited to:

—*Whole Body Imaging Technology.*—TSA continues to examine the feasibility of using a whole body imaging technology to improve the detection of explosives and prohibited items on persons. Ongoing efforts with two vendors has led to the development of a device that is capable of producing a generic body image that effectively highlights security threats on persons while not unduly infringing on their privacy. TSA is currently working on the details for the pilot phase,

including vendor capabilities to support a timetable, selection of the pilot locations, and the operating policy for screening with this technology.

—*Explosives Detection System (EDS) for carry-on baggage.*—TSA has conducted preliminary evaluations of an automated EDS for carry-on baggage and is currently collecting engineering data with the unit to promote further development. This technology will automate the detection of explosives in carry-on baggage, similar to the capabilities TSA has achieved for checked baggage screening. Simultaneously, we have a robust ongoing R&D project to develop a technology that will automate the search not only for explosives in carry-on baggage, but for weapons as well.

—*Cast and Prosthetic Device Scanner.*—TSA is working to develop a technology solution to more effectively screen cast and prosthetic devices for weapons and prohibited items. TSA expects to pilot the technology in the first quarter of fiscal year 2006.

—*Explosives Detection Bottle Scanners.*—TSA is working with industry to evaluate the effectiveness of bottle scanners to screen for liquid explosives. TSA has issued a solicitation to industry to submit products for lab evaluation.

NATIONAL CENTER FOR CRITICAL INFORMATION PROCESSING AND STORAGE

Question. The National Center for Critical Information Processing and Storage at Stennis Space Center performs the important function of providing a secure and reliable system to process, manage, and secure data for the Federal Government. Could you update us on the status of that project?

Answer. Construction of the DHS data center at Stennis Space Center has been delayed. The Naval Oceanographic Office had been experiencing difficulties issuing a construction contract prior to Hurricane Katrina. The Naval Oceanographic Office now reports that, due to Hurricane Katrina, work crews are not available for the limited construction effort that is under contract (demolition and roofing). The delay to the project is not yet fully quantifiable. The DHS construction effort must now compete for resources with regional reconstruction efforts.

Question. Specifically, when will the additional $30 million of fiscal year 2005 be available for build-out and construction at Stennis?

Answer. The Stennis Procurement Package was released by DHS on May 13, 2005.

QUESTIONS SUBMITTED BY SENATOR TED STEVENS

TRANSPORTATION OF BUTANT STOVES (WITHOUT BUTANE) ON AIRPLANES

Question. Constituents have contacted me to complain about TSA. Alaskans have attempted to carry on butane stoves onto airplanes within their luggage. The stoves, although no butane was present, were confiscated by TSA. These stoves are used for camping and general use in rural Alaska; the stoves do not pose a threat to anyone on a plane.

Why is TSA disallowing passengers from carrying butane stoves, without butane, in their luggage?

Answer. Under regulations issued by the Federal Aviation Administration (FAA), there are restrictions in place on the transport of hazardous materials on board any aircraft. With regard to the transportation of butane stoves as checked baggage, in accordance with the baggage screening standard operating procedure (SOP), if a TSA screener finds a stove that potentially has fuel inside, an airline employee is notified so that a determination may be made regarding the contents of the stove. Typically, the airline employee removes the fuel bottle(s) from the stove, after which the stove can be transported in checked baggage. If the fuel bottle cannot be removed, in general, it will not be allowed to be transported. In some small locations in Alaska where the transport of camp stoves is prevalent and it is relatively easy to contact the passenger, the airline employee will contact the passenger and give that person the option to empty and clean the bottle before accepting the stove for transport. However, an unused camp stove still in the box with no fuel or emanating fumes should not be refused transport.

FISHERIES ENFORCEMENT

Question. I'm informed the Coast Guard plans to deploy C–130s to Shemya or Galena to increase surveillance and enforcement of fisheries laws inside the Maritime Boundary Line. A report issued in 2004 indicated the Coast Guard could not render its deployment throughout the high threat season because of the lack of facilities in the Aleutians. Last year, I included language in the Homeland bill to direct the

Coast Guard to include in its budget submission the funds necessary to provide support facilities for Shemya, Galena, Cold Bay and other western Aleutian Islands. The Coast Guard was not able to follow Congressional direction and the costs were not included in the budget submission.

What are the costs estimates associated with this problem?

Answer. Increased regulation and management on the Russian side of the Maritime Boundary Line (MBL) have significantly decreased the need to forward deploy C–130 aircraft for MBL patrols. MBL enforcement flights originating from Air Station Kodiak are proving effective. At the same time, the need for forward-deployed HH–60's appears to be increasing to meet search and rescue and fisheries enforcement mission needs in Western Alaska waters.

HH–60 forward deployments often occur from locations such as Dutch Harbor, Cold Bay and St. Paul Island. Although highly effective, these forward deployments often present our crews with challenging conditions because of sub-standard facilities—and inadequate commercial infrastructure to properly support these deployments. Addressing these deficiencies is a Coast Guard priority.

The Coast Guard recently initiated a formal planning effort to develop alternatives and identify resources needed to respond to these changing mission needs. Most of these facilities are not Coast Guard-owned, so innovative public-private partnerships may be necessary to allow infrastructure improvements. The Coast Guard will keep the Committee advised of progress on this planning effort. The Coast Guard can not accurately predict costs at this early stage in the planning process.

UAVS

Question. What are the Coast Guard's plans for using Predator medium endurance unmanned aerial vehicles for fisheries enforcement and search and rescue activities in Alaska?

Answer. The Coast Guard has no immediate plans to use Predator unmanned aerial vehicles (UAVs) for operational service in Alaska. The recent proof of concept exercise demonstrated promise for a maritime-configured UAV, but identified shortcomings must be addressed to make this a Coast Guard mission capable asset. Among the technical challenges that still must be resolved are reliable communications and aircraft control at high latitudes, integration of on-board sensors, limited all-weather operations (including icing and crosswind limits), and compliance with Federal Aviation Administration air control requirements.

UAVs remain a critical future element of the Coast Guard's Deepwater program. The Coast Guard is partnering with other DHS and DOD agencies to carry out further evaluation programs and take advantage of technology improvements that will ultimate make UAVs suitable for use in the maritime environment.

Question. Does the Department plan to utilize the two previous Alaskan UAV demonstrations for further testing in Alaska or Hawaii?

Answer. DHS is working with the DOD to plan additional UAV testing in all operational environments to demonstrate the UAV concept to support a variety of missions. A cooperative effort between the National Oceanic and Atmospheric Administration (NOAA) and the Coast Guard to test UAV use in Hawaii, combining scientific research with maritime sensor validation, was recently cancelled due to lack of NOAA funding. The Coast Guard will continue to establish partnerships that may yield opportunities for future Hawaii-based testing.

Further demonstrations in Alaska can be planned when UAV technology matures to resolve the key issues of reliable communications and aircraft control at high latitudes and all-weather operations (including icing and crosswind limits). Prior Coast Guard UAV testing in Alaska has demonstrated that these limitations restrict UAV operations in Alaska.

Question. Does the Department have any plans to use UAV's to help TSA provide surveillance to non-aviation modes of transportation such as the Trans Alaska Pipeline System?

Answer. UAVs offer a range of capabilities that are suitable throughout DHS. The UAV capability for 24-hour, all weather surveillance is particularly useful in border security applications, critical infrastructure protection, transportation security, or in support of U.S. Coast Guard (USCG) maritime domain awareness missions. In April 2004, the DHS/UAV working group submitted a report to Congress addressing the applicability of UAVs in various homeland security applications.

As part of a USCG Predator 2 UAV demonstration in July 2004, TSA coordinated with the USCG to fly over designated sites on the Trans Alaska Pipeline (TAPS). The purpose of the TAPS demonstration was to evaluate the effectiveness and practicality of the UAV and associated sensors for pipeline surveillance. This effort pro-

vided additional evidence of the utility of UAVs as part of a layered surveillance effort. TSA will continue to evaluate the use of UAVs with regard to pipeline surveillance and looks forward to working with Congress on the issue.

QUESTIONS SUBMITTED BY SENATOR PETE V. DOMENICI

BORDER NEEDS—SECURITY UPDGRADES AT PORTS

Question. America has 197 land ports of entry, and it has been almost 20 years since we launched a major effort to upgrade infrastructure at those ports. That last effort occurred in 1986, when former Senator DeConcini and I developed the Southwest Border Improvement Program to improve border infrastructure so that States could better take advantage of commerce and trade opportunities with Mexico. That was almost 15 years prior September 11, 2001.

Since September 11, we have placed increasing emphasis on upgrading security for our airports, seaports, and critical infrastructure. It is imperative that we also improve land port security. To that end, I will introduce a bill authorizing additional funds for investment in our nation's border crossings.

Have you considered what kinds of improvements are necessary at our land ports of entry and how much these upgrades might cost?

Answer. DHS is in the midst of a systems-level review of its border control architecture to identify the right mix of personnel, technology and infrastructure to help achieve effective control of the border. DHS will identify a program manager to oversee the development of a specific set of border security plans. The Department will be in a better position to comment on this question following the conclusion of this review.

Question. Specific improvements are needed at the Columbus port of entry in New Mexico, and the General Services Administration (GSA) has proposed construction on the Columbus project to begin in 2007 or 2008. Do you support GSA's recommendation and will you make every effort to keep the project on track for construction?

Answer. As noted above, DHS is in the midst of a systems-level review of its border control architecture. This review is intended to help the Department identify the right mix of personnel, technology and infrastructure to help achieve effective control of the border. The Department will be in a better position to comment on this question following the conclusion of this review.

BORDER NEEDS—UAV TECHNOLOGY

Question. In last year's intelligence reform bill, I called for the Department of Homeland Security to develop a plan for using Unmanned Aerial Vehicles ("UAVs") on America's southwest border.

In New Mexico, we have some experience with UAVs because our university near the southwestern U.S. border operates a UAV validation and test facility sponsored by the Department of Defense. Because of the established presence of UAVs at New Mexico State University, and because of our location as a border state, I believe New Mexico would be an asset in the use of UAVs for surveillance.

What are your views concerning the use of UAVs for securing remote areas of our borders?

Answer. As noted above, DHS is in the midst of a systems-level review of its border control architecture. DHS is also currently working to begin the process of procuring UAVs. The Department's objective is to get that done in a matter of months and start to deploy UAVs and have them flying over the border. That said, DHS cannot rely exclusively on UAVs, and manned vehicles and helicopters will also play a role.

Question. How many UAVs does DHS currently own?

Answer. As of August 20, DHS currently does not own any UAVs.

Question. Where are these UAVs stationed?

Answer. As of August 20, DHS currently does not own any UAVs.

Question. Will your staff evaluate evaluate the existing UAV facility at New Mexico State University and the Las Cruces International Airport as a potential home for the Department's UAV program?

Answer. As noted above, DHS is in the midst of a systems-level review of its border control architecture. The Department will be in a better position to comment on this question following the conclusion of this review.

BORDER PERSONNEL—MANPOWER

Question. As you know, adequate staffing at our nation's land ports of entry is essential for the safety of parties involved in the flow of traffic across the border and for efficient commerce.

Last year's legislation that reorganized our intelligence community called for an increase in border patrol agents, and President Bush's fiscal year 2006 budget requests funds to hire an additional 210 agents.

Have you studied where placing these agents would be most beneficial?

Answer. Emergency Supplemental Legislation and President Bush's fiscal year 2006 Budget call for the hiring of an additional 710 agents by the end of fiscal year 2006, and CBP is taking aggressive steps to recruit, hire and train candidates to fill these spots. The hiring of these new agents comes in addition to the standard attrition hires that supplement the several hundred agents who retire, transfer, or leave for medical reasons over the course of a year. New agent positions will be allocated based on risk-based priorities.

Question. When might these new agents be hired and put in place?

Answer. There is currently an open recruiting announcement to obtain additional potential new employees.

Question. How can we better retain existing border patrol officers so that as we place these new agents along our borders, we are not losing agents with experience?

Answer. CBP is currently examining methods that can be used to retain seasoned agents. The current attrition rate for experienced agents (GS–9 and higher) is less than 5 percent.

BORDER PERSONNEL—TRAINING AT FLETC

Question. One of the Federal Government's premier training sites for law enforcement officers is located in New Mexico. Many Federal law enforcement officers have trained at the Federal Law Enforcement Training Center in Artesia (FLETC-Artesia), including Air Marshals and Federal Flight Deck Officers.

Additionally, both basic and advanced training for Border Patrol Agents is now conducted at FLETC-Artesia. I lauded the Department's decision to consolidate border patrol training in Artesia because it makes sense to have all training at one facility. Additionally, training border patrol officers in a border State gives trainees a first-hand look at the area they are charged with protecting.

What, if anything, does the Department need from FLETC-Artesia?

Answer. FLETC is proceeding to put into place the temporary structures and staffing directed in the recently enacted fiscal year 2005 Supplemental. As more information and details are developed on additional training needs we will keep the Congress apprised.

Question. Has DHS considered taking border patrol trainees to the Mexico border as part of their overall training?

Answer. FLETC uses scenario base training utilizing Spanish speaking role players in a controlled environment identical to that seen on the southwest border. This scenario based training affords trainees the opportunity to correct mistakes and become comfortable with assigned duties prior to assignment in a U.S. Border Patrol sector. This system of training is more flexible and less costly than providing visits during basic training to border sites. The Border Patrol also employs a system of supervision and on-the-job experience for newly graduated agents.

Question. If new facilities were constructed at FLETC-Artesia, would you support legislative language to streamline the design, engineering and construction of those facilities?

Answer. The Department is always open to considering legislative methods that streamline and improve our processes while promoting full and open competition.

NEW MEXICO CAPABILITIES—TRAINING AT PLAYAS

Question. Secretary Chertoff, last fall New Mexico Tech opened the Playas Training Center. DHS played an integral part in this center by providing the funding for New Mexico Tech to purchase Playas, a small town in Southwest New Mexico that was virtually abandoned when the copper smelting operation in the area was shut down in 1999.

Playas' remote location and open space makes it an ideal place for New Mexico Tech to develop a wide range of research and training activities to support homeland security efforts nationwide.

What new training activities could DHS use at Playas?

Answer. It is my understanding that Playas will be jointly developed by the New Mexico Institute of Mining and Technology and the New Mexico State University.

As you are aware, ODP has funded the New Mexico Institute of Mining and Technology since fiscal year 1998 as part of the National Domestic Preparedness Consortium. As part of the Consortium, the New Mexico Institute for Mining and Technology supports ODP's mission of assisting State and local governments plan and prepare for incidents of domestic terrorism by providing critical training to the Nation's first responders. The State of New Mexico used State funds rather than Federal homeland security funds to purchase the Playas Training Center. Nevertheless, ODP does have a use agreement in place with New Mexico Tech to use the Playas Training Center over a 5-year period. As the Playas Training Center is further developed, the Department's ODP will coordinate with New Mexico Tech officials to determine the types of training initiatives that could be supported by the Playas Training Center.

Question. How much is included in the President's fiscal year 2006 budget for training first responders?

Answer. The fiscal year 2006 President's Budget request for SLGCP includes over $83 million for the State and Local Training Program. Through this funding, SLGCP will continue to develop and deliver state-of-the-art training programs through its coalition of "Training Partners." This coalition, comprised of government facilities, academic institutions and private organizations provide a variety of specialized training for emergency responders across the country. The fiscal year 2006 funding request will support SLGCP's Continued and Emerging Training Program, the Center for Domestic Preparedness, and the National Domestic Preparedness Consortium. In addition, a portion of SLGCP grants to States and urban areas are also devoted to training.

FEMA also conducts an extensive array of training for emergency personnel through the National Fire Academy, the Emergency Management Institute, and the Noble Training Center with a budget that totals approximately $15 million. Other DHS components, such as the Federal Law Enforcement Training Center, also provide training for selected State and local personnel.

Question. What are your thoughts on providing standardized training for all first responders, at both the Federal and local level, in a facility like the one at Playas?

Answer. The New Mexico Institute of Mining and Technology, including its training facility at Playas, already supports ODP's training efforts through the National Domestic Preparedness Consortium. As such, these facilities will comply with all training standards required for ODP training.

Standards for training encompass the instructional design of the training, the quality of training content, the effectiveness of the instructors, as well as successful knowledge transfer measured through student evaluation. With respect to development of training programs, the ODP Training Division has adopted the industry standard instructional systems design approach of analysis, design, development, implementation, and evaluation (ADDIE) as detailed in the ODP Strategy for Blended Learning. The ADDIE approach for instructional design ensures a valid training need is identified, the most effective methodology for instruction is identified, and training content is monitored for accuracy and effectiveness throughout the process.

The development of training content based on effective needs analysis is also based upon performance standards. DHS efforts in this area related to training for emergency responders began with the ODP Training Strategy developed in 2002, which provided guidance on who should be trained to perform what tasks, using what methodologies to maximize training efficiencies. The strategy further addressed effective methods for evaluating competency and performance after training was completed and what gaps needed to be remedied. This work led to the ODP-developed Emergency Responder Guidelines, which were promulgated in August 2002. These are currently undergoing revision to reflect a broader range of response disciplines and the private sector.

Additionally, as the executive agent for the development and implementation of HSPD–8, "National Preparedness," SLGCP has developed and promulgated an Interim National Preparedness Goal (NPG). The Interim NPG, which was released on March 31, 2005, was developed using capabilities-based planning. Capabilities are combinations of resources that provide the means to achieve a measurable outcome resulting from performance of one or more critical tasks, under specified conditions and performance standards. The Target Capabilities List identifies 36 Target Capabilities and is currently available.

ODP's Training Division, along with our training partners, is in the process of examining the capabilities associated with the national priorities included in the Interim National Preparedness Goal to align training curricula to these national priorities and the related capabilities. It is the Department's goal and expectation to have its training courses aligned with the national priorities in fiscal year 2006.

Further, with respect to professional standards, ODP requires its training partners, State Administering Agencies, and Federal partners to adhere to and incorporate the following professional standards in training curricula to which they are applicable:

—29 Code of Federal Regulation (CFR)1910.120, Hazardous Waste Operations and Emergency Response;
—29 CFR 1910.134, Respiratory Protection;
—National Fire Protection Association (NFPA) 471, Recommended Practice for Responding to Hazardous Materials Incidents;
—NFPA 472, Professional Competence of Responders to Hazardous Materials Incidents;
—NFPA 473, Standard for Competencies for EMS Personnel Responding to Hazardous Materials Incidents;
—NFPA 1006, Standard for Rescue Technician Professional Qualifications;
—NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs 2004, specifically Chapter 5, section 5.12; and
—NFPA 1670, Standard on Operations and Training for Technical Rescue and Search Incidents.

Question. Will the Department work to make State homeland security directors aware of the Playas Training Facility in an effort to help local first responders receive adequate training?

Answer. ODP is undertaking a web-based information portal initiative, the First Responder Training portal, that will be the primary location for information and resources serving the first responder community in support of the DHS strategic goal of improving the nation's ability to prevent, prepare, mitigate, respond to, and recover from emergency situations and events. The portal will create a functional tool to support the development and delivery of efficient, effective and consistent first responder training. Registered under the domain name of firstrespondertraining.gov, the website will provide a single, authoritative link for the first responder community and will include collaboration tools and information on training, grants, equipment, and standards.

This portal will complement FEMA/U.S. Fire Administration's (USFA) existing on-line training portals, the Emergency Management Institute's Independent Study website, and the USFA National Emergency Training Center (NETC) Virtual Campus, which together offer more than 60 courses for emergency personnel and has registered more than 350,000 course completions already this fiscal year. The NETC Virtual Campus courses are intended for Federal, state, and local officials including emergency management personnel, fire service personnel, police, public works, health officials and first responders, and also DHS personnel, and the general public.

The ODP First Responder Training portal and FEMA's on-line training facilities will provide consistent delivery of training to large audiences and will be used as a delivery mechanism by our partners to continue to enhance the capacity of the emergency responder community. Additionally, this web-based training will: accommodate students with disabilities by use of assistive technologies; be designed to support small group work and collaboration; provide multi-purposed training and resources; have the capability to restrict access to only authorized users; offer students the opportunity to remediate materials until proficient or "opt out" of content they have already mastered; and be linked through other initiatives currently underway to track user activity and accurately provide student transcripts.

The framework and inter-workings of the overall system are nearing completion. A pilot test, testing functionality and usability for internal users/developers (training partners) and external users (students from the first responder communities), will begin in June 2005. Results from the pilot test will be used to make improvements to the system and to determine the effectiveness of the technology in support of ODP's National Training Program.

Prior to the development of the First Responder Training portal, ODP developed a Training Course Catalog, as well as comprehensive guidelines associated with attending ODP-sponsored training courses. This information is available to the Nation's first responder community through a number of different means, including ODP's publicly-available website (http://www.ojp.usdoj.gov/odp) as well as through routine interaction with ODP's State Preparedness Officers and the nation's first responder community. As New Mexico Tech develops training courses at Playas Training Center, ODP will make this information available through its various outreach mechanisms, including the First Responder Training portal.

New Mexico Capabilities—Dirty Bomb Training

Question. New Mexico Tech has also joined with New Mexico State University ("NMSU") to propose an expansion of the anti-terrorism training program for first

responders. This expansion would include a course about radiological dispersal devices (also known as dirty bombs).

I believe this proposal has merit because the aftermath of a dirty bomb attack is one of our gravest anticipated terrorist attacks, and our first responders need appropriate training to respond to such a threat. New Mexico Tech and NMSU's Carlsbad Environmental Monitoring and Research Center have the scientific expertise, radiological handling capabilities, radioactive material license, and trained staff to address both the scientific and training aspects of dirty bombs, and collaboration between these universities and New Mexico's national nuclear weapons labs could provide ideal training first responders to counter dirty bomb risks.

What dirty bomb training do Federal first responders currently receive?

Answer. FEMA/USFA's Emergency Management Institute (EMI), as well as the National Fire Academy, offers a full range of courses that prepare state, local, and tribal emergency personnel to deal with the aftermath of all types of events involving radiological materials. EMI courses such as "Radiological Emergency Response Operations" and "Advanced Radiological Incident Operations" and the NFA's Command and Control of Emergency Incidents provide specific instruction in how to prepare for such events.

Although there is no specific course dedicated to radiological dispersal devices, several courses delivered by members of the National Domestic Preparedness Consortium (NDPC) cover radiological dispersal devices in their course curriculum. The extent to which radiological dispersal devices are covered in the various courses ranges from a five minute overview to a detailed 2.5 hour block of instruction. States, territories, and urban areas may use SLGCP-certified training to enhance the capabilities of State and local emergency preparedness and response personnel as it adheres to the State's Homeland Security Strategy. The target audience for SLGCP-certified training courses includes State and local emergency preparedness, prevention and response personnel; emergency managers; and public/elected officials within the following disciplines: fire service, law enforcement, emergency management, emergency medical services, hazardous materials, public works, public health, health care, public safety communications, governmental administrative, cyber security, and private security providers.

Question. Could New Mexico Tech's training facility in Playas, New Mexico be the ideal place to base such training?

Answer. As you are aware, ODP has funded the New Mexico Institute of Mining and Technology since fiscal year 1998 as part of the National Domestic Preparedness Consortium. As part of the Consortium, the New Mexico Institute for Mining and Technology supports ODP's mission of assisting State and local governments plan and prepare for incidents of domestic terrorism by providing critical training to the nation's first responders. ODP periodically reviews its training requirements and builds on the strengths of its training partners. Currently, nuclear and radiological training primarily falls under the Department of Energy's Nevada Test Site (NTS). However, ODP will review any unique capabilities the Playas Training Center may offer.

RESEARCH AND TECHNOLOGY—GENERALLY

Question. The Department of Homeland Security has used many different resources to implement innovative protective measures across the country. We have improved security nationwide through the Department's Science and Technology Directorate, the Advanced Research Projects Agency, Centers of Excellency, and similar divisions and initiatives.

The Department's leadership in developing innovative tools and technologies to protect our Nation is one of the most important roles the Department plays. However, with so many groups working on developing new technologies, it may prove difficult to select the best technology available.

How does DHS intend to most effectively integrate and leverage existing efforts and capabilities to ensure that the best technologies available are utilized?

Answer. Last year, the S&T Directorate developed and documented a robust RDT&E process. The goal of the RDT&E process is to provide a clearly defined, repeatable method for assessing needs and risk, planning, allocating resources and executing programs to produce high-impact, cost-effective and critically needed homeland security technology solutions.

The S&T Directorate's RDT&E process uses a risked-based approach to planning and identifies critical capability gaps before attempting to identify or develop technology solutions. In developing solutions, the process engages the end-user throughout requirements definition, development, testing and transition. The process considers the product life cycle from the outset, including planning and budgeting for

production, deployment, operations and support. It is this process which allows us to prioritize both within and across fields.

Integration of existing efforts and capabilities occurs in several key areas. For example, the S&T Directorate collaborates with academia through the Centers of Excellence program and its associated Integrated Network of Centers, which is establishing a national network of affiliated universities. Additionally, the S&T Directorate has a sizeable number of interactions and programs with individual universities on specific research topics and needs.

The S&T Directorate also maximizes and leverages the existing capability base of the national laboratory complex. The Directorate engages all the national laboratories on a case-by-case basis, to tap into unique technical expertise that is critical to accomplishing portfolio objectives and goals. The Directorate also relies on national laboratory technical experts as needed throughout the RDT&E processes based on their years of experience applying technologies and processes to field applications. This technical and practical expertise is used to accelerate spiral development of technologies for transitioning capabilities to operational end-users.

The S&T Directorate solicits proposal from industry and uses a full range of contracting vehicles and its authority under the Homeland Security Act to engage businesses (large and small), Federally funded research and development centers, universities, and other entities in development of advanced technologies for homeland security. The contracted research and development work now underway is the S&T Directorate's main form of collaboration with industry and academia.

Question. Under your leadership, how will the Science and Technology Directorate collaborate with academia, industry and our national labs?

Answer. The S&T Directorate collaborates with academia through the Centers of Excellence program and its associated Integrated Network of Centers, which is establishing a national network of affiliated universities. Additionally, the S&T Directorate has a sizeable number of interactions and programs with individual universities on specific research topics and needs.

The S&T Directorate solicits proposals from industry and uses a full range of contracting vehicles and its authority under the Homeland Security Act to engage businesses (large and small), Federally funded research and development centers, universities, and other entities in development of advanced technologies for homeland security. The contracted research and development work now underway is the S&T Directorate's main form of collaboration with industry and academia.

The S&T Directorate maximizes and leverages the existing capability base of the national laboratory complex. The Directorate engages all the national laboratories on a case-by-case basis, to tap into unique technical expertise that is critical to accomplishing portfolio objectives and goals. The Directorate also relies on national laboratory technical experts as needed throughout the RDT&E processes based on their years of experience applying technologies and processes to field applications. This technical and practical expertise is used to accelerate spiral development of technologies for transitioning capabilities to operational end-users.

The S&T Directorate engages all the national laboratories on a case-by-case basis, to tap into unique technical expertise that is critical to accomplishing portfolio objectives and goals. The Directorate also relies on national laboratory technical experts as needed throughout the RDT&E processes based on their years of experience applying technologies and processes to field applications. This technical and practical expertise is used to accelerate spiral development of technologies for transitioning capabilities to operational end-users.

For example, the Countermeasures Test Beds (CMTB) program operates in close partnership with a number of Federal and national laboratories to execute its mission of testing and evaluating all threat countermeasures and systems. The following national labs participate in all CMTB Operational Testing and Evaluation (OT&E) efforts and enable deployments in response to heightened alert conditions as necessary. Multi-lab teams are encouraged to ensure objectivity and a healthy interchange of ideas.

As another example, the Office of Interoperability and Compatibility (OIC) is currently leveraging the resources of Eastern Kentucky University in developing effective test methodologies for equipment and to provide technical assistance to States and localities under the SAFECOM Program. At the same time, OIC has enlisted a consortium of well over one hundred universities and colleges to support the annual conference on Technologies for Public Safety in Critical Incident Response, jointly sponsored by DHS and the DOJ. Industry associations participate in SAFECOM Program activities, especially in standards development efforts. OIC has established a monthly vendor process which allows for constant communication and collaboration with our industry partners. Additionally, OIC/SAFECOM will be conducting an industry summit in late fall to allow for ever greater collaboration.

Additionally, the BioSecurity program currently works closely with academia, industry and the national labs to fulfill its national mission.

Question. How will you allocate funding to national laboratories, universities, and industry in a competitive and transparent manner?

Answer. The S&T Directorate supports seeking the best sources to accomplish DHS RDT&E goals through full and open competition.

Individual national laboratories have recognized expertise in specific technical fields built up from years of experience in national defense technology development. Recognizing those areas of expertise, integrated technical programs have been formed from multiple laboratories to solve problem sets related to their expertise. The laboratories assist in leading the formation of the technical teams addressing specific problem sets. The S&T Directorate uses a performance based approach to ensuring quality programs. As such, annual external reviews are conducted with subject-matter experts and end-user reviewers to evaluate the performance and outcomes of individual programs. Results from these reviews are documented and used to inform decisions on the next fiscal year's program execution plans.

All funds allocated by University Programs to universities and individuals at universities are the product of a highly competitive merit-based selection process. A large number of subject matter experts from government, industry and academia use well-established and documented peer review selection procedures in making funding recommendations.

All S&T Directorate Broad Agency Announcements and Small Business Innovation Research solicitations are public and competitive. All are published on the official Federal Government procurement website (and simultaneously on the S&T Directorate's HSARPA websites) and each contains explicit instructions on how to submit white papers and proposals. The criteria by which these submissions will be evaluated for technical merit are published in each solicitation. The source selection plan which guides the panel of experts who evaluate the submissions is approved at the same time the solicitation is published and records of their final decisions are retained. Selections for funding are typically made on technical merit, relevance to DHS mission, available funding, and programmatic considerations by a source selection authority.

Also, the S&T Directorate works to ensure all of its program offices allocate funding to national and Federal laboratories, universities, and industry where appropriate, following the competitive guidelines outlined in the Federal Acquisition Requirements. The S&T Directorate continually monitors all program aspects to determine best value and cost effectiveness. As the S&T Directorate works to mature and transition mature technologies to the user community, a competitive process is used.

RESEARCH AND TECHNOLOGY—NISAC

Question. The National Infrastructure Simulation and Analysis Center, or NISAC, is funded by DHS to evaluate the effects of disruptions to America's infrastructure, and much of NISAC's work is done by New Mexico's two National Laboratories: Sandia and Los Alamos.

I strongly believe in NISAC's efforts and capabilities, but I do not believe the program is being used by the entire Department of Homeland Security to its full extent.

What are your plans to coordinate the Department's Directorates so NISAC is utilized by the entire Department?

Answer. The Department's National Infrastructure Simulation and Analysis Center (NISAC) is a program in the DHS IAIP Directorate. Since its inception, NISAC has had the mission to provide comprehensive modeling and simulation capabilities for the analysis of critical infrastructures, their interdependencies and complexities, and the consequences of disturbances. This mission and NISAC's expertise directly support the modeling, simulation, and analysis initiatives of DHS. For fiscal year 2005, IAIP will continue to expand NISAC's operational development of a suite of infrastructure modeling, simulation and analytic capabilities with an emphasis on interdependencies and consequences of infrastructure disruptions for the Nation as a whole.

At present, IAIP is coordinating ongoing NISAC work with the S&T Directorate, the Coast Guard, FEMA, BTS, and TSA, as well as with the Departments of Transportation and Energy, on multiple projects that concern the nation's infrastructure. The NISAC program office will continue its efforts to broaden the awareness of the NISAC program throughout DHS to ensure this national resource is properly tasked with the most urgent and complex problems concerning infrastructure dependencies and interdependencies. IAIP will continue to fully utilize, and if warranted expand, the existing capabilities of NISAC with IAIP acting as the central coordinator for

NISAC efforts in keeping with IAIP's national charter of coordinating and leading efforts for the understanding and protection of the nation's infrastructure. Moreover, as the Department's ability to execute risk assessment continues to mature, NISAC will become more and more integrated into the full range of Federal risk management programs.

Question. How will you work with the Director of National Intelligence to make NISAC's capabilities available to the intelligence community through a formal relationship, as required by last year's intelligence reform bill?

Answer. IAIP is continually improving the integration between the organizations that develop the three components of our Strategic Risk Analysis; which are consequence, vulnerability and threat or attractiveness. A prime example of this effort is ensuring that the intelligence component of DHS, the Office of Information Analysis, currently in IAIP, is aware of NISAC's capabilities and, as a byproduct, the resident expertise at the national laboratories. As the NISAC products are more fully developed and matured, this integration will increase.

As a continuation of this integration, we will engage with the Director of National Intelligence to make him aware of a variety of efforts the Department has underway that will benefit from his efforts, NISAC included. We will seek a formal relationship for information and capability sharing as warranted, between non-DHS elements of the intelligence community and the Department, including the NISAC.

Question. What do you need from Congress to fully implement NISAC's capabilities?

Answer. Congress's continued support for all of the Department's programs that seek to reduce the risk of terrorism to the Nation are greatly appreciated. All of these programs are essential, including the Department's National Infrastructure Simulation and Analysis Center.

RESEARCH AND TECHNOLOGY—DOMESTIC NUCLEAR DETECTION OFFICE (DNDO)

Question. The Department has a new office tasked with deploying radiation detection technologies and systems designed to detect attempts to smuggle nuclear materials or weapons into the United States. As such, the Domestic Nuclear Detention Office, is likely to play a critical role in testing and evaluating current and next generation technologies to assure that DHS agencies have the most effective and accurate tools.

How does DNDO intend to balance the needs between rapidly deploying detection systems and developing technologies that can best fulfill its mission?

Answer. The DNDO will include, as part of its staff, an Office of Systems Engineering, which will be dedicated to development of the global systems architecture, as well as a comprehensive systems engineering capability. This office will be tasked with providing quantifiable analysis of issues such as this and providing cost-benefit analysis, when appropriate, to determine the relative advantages gained by deploying current technologies or developing additional capabilities.

Additionally, beyond the DNDO office structure, the DNDO will also utilize the Department's robust, two-tiered validation process for large-scale programs, consisting of a Joint Requirements Council and an Investment Review Board, which have final approval to authorize deployment or development programs.

Question. How do you plan to develop and support the nuclear facilities and infrastructure needed to test and evaluate evolving technologies, missions, and operational concepts?

Answer. The DNDO will continue to proceed with the design and construction of the Radiological and Nuclear Countermeasures Test and Evaluation Complex (RadNucCTEC) at the Nevada Test Site. The construction of this facility, begun within the DHS S&T Radiological and Nuclear Countermeasures portfolio, will bridge the gap between "bench-top testing" performed by developers and operational field testing conducted during pilot deployments, providing the unique capability to test systems in a near real-world environment against actual special nuclear materials in authentic configurations. Construction is expected to begin in June 2005 and be completed by the end of fiscal year 2006.

Additionally, DNDO will continue to utilize the DHS S&T Countermeasures Test Bed (CMTB) for operational testing and evaluation. CMTB will provide a critical, objective testing environment to evaluate technologies and concepts of operation for nuclear and radiological detection in key operational venues.

Question. With the creation of DNDO, will the efforts to prevent and respond to radiological dispersion devices be retained in the Science and Technology Directorate, moved into DNDO, or shared between these two DHS divisions?

Answer. Many experts consider a nuclear attack to be less likely than the release of a radiological dispersion device (RDD). However, a nuclear attack would be many

times more devastating than one employing an RDD, both in terms of economic impact and casualties. While the primary focus of DNDO is, therefore, to develop and acquire systems and capabilities for the detection of special nuclear materials (SNM) and nuclear devices, most nuclear threat detection systems will also detect radiological threats, because of the similarity in nature of radioactive signatures of special nuclear materials nuclear devices and radiological materials usable in an RDD.

As such, the division of responsibilities for prevention and response for RDDs between DNDO and the S&T Directorate is the same as that for nuclear devices or materials. DNDO will be responsible for the development of the detection architecture, as well as the systems to be deployed, for the prevention of an attack. Additionally, DNDO will be responsible for the development of training and response protocols in the event of an alarm. However, DNDO will not be responsible for the development of incident management or decontamination technologies; these programs will remain in the S&T Directorate.

Question. What role will national weapons labs play in DNDO?

Answer. DNDO will continue to work with the Office of National Laboratories in the S&T Directorate to make sure that work is properly coordinated and that all of the national laboratories, including the weapons labs, receive clear guidance and direction on efforts they conduct with DNDO or the S&T Directorate.

DNDO recognizes that the national weapons laboratories have long been one of this nation's preeminent sources of critical nuclear expertise. That expertise, along with the expertise found in academia and industry, will be vital to responding to the threat posed by nuclear and radiological weapons or materials and in developing transformational capabilities to significantly enhance the U.S. capability to protect against this threat.

QUESTIONS SUBMITTED BY SENATOR ROBERT C. BYRD

DRUG TRAFFICKING

Question. The President has said, "trafficking in drugs finances the work of terrorists, sustaining terrorists and that terrorists use drug profits." Given the President's view, I am surprised that he has included almost no initiatives in your budget to disrupt the drug trade. Why?

Answer. The fiscal year 2006 President's Budget includes $3.455 billion that affects or may affect the counternarcotics activities of the Department or any of its subdivisions, or that affects the ability of the Department or any subdivision of the Department to meet its responsibility to stop the entry of illegal drugs into the United States.

Within that $3.455 billion total, approximately $2.937 billion has been identified as National Drug Control Budget Funds—funds for those Department programs and initiatives that directly support Priority III of the President's National Drug Control Strategy (Disrupting the Market: Attacking the Economic Basis of the Drug Trade). This funding will provide the Department with resources to strengthen and focus its illegal drug market disruption efforts while, at the same time, dedicating new resources for emerging threats. In addition to these funds, approximately $480.5 million has been identified as other potential expenditures that also may affect the counternarcotics activities of the Department.

These funds support counternarcotics programs and counternarcotics-related activities that can build on the Department's many accomplishments towards stopping the entry of illegal drugs into the United States.

LOBBYING RULES

Question. On November 23, the Office of Government Ethics, in response to a Department of Homeland Security (DHS) request, relaxed lobbying prohibitions for former "senior employees" of the Department. Up until November 23 of this year, any former "senior employee" of DHS was barred from lobbying any individual or office in DHS for 1 year. A senior employee is any individual whose rate of basic pay is equal or greater than 86.5 percent of the rate for level II of the Executive Schedule. The 2004 salary for an Executive Level II employee is $158,100, 86.5 percent of which is $136,756.

The revised rule by the Office of Government Ethics designates seven distinct and separate components in DHS for purposes of 18 U.S.C. 207(c), which covers conflict of interest restrictions for senior Federal officials in post-employment. The components designated are: Transportation Security Administration (TSA); Coast Guard; Secret Service; Federal Law Enforcement Training Center (FLETC); Science &

Technology (S&T) Directorate; Information, Analysis & Infrastructure Protection (IAIP) Directorate; and Emergency Preparedness & Response (EP&R).

By designating seven distinct and separate components in DHS, any former official who worked in one of those seven components is now permitted to immediately lobby anywhere in DHS except for the component for which they were employed. It also allows senior officials who worked for DHS, but not in one of the seven designated components, to immediately lobby anyone in those components designated as distinct and separate. For instance, a senior employee who worked in the Office of the Secretary for Tom Ridge can immediately lobby any of the DHS organizations cited above. Those seven components alone comprise over $19 billion and nearly 60 percent of the Department's funding.

Why did DHS request this change to the lobbying rules?

Answer. The recommendations were made to appropriately tailor the application of the 1-year cooling-off restriction to the circumstances existing within the newly created Department of Homeland Security. Section 207 of title 18 of the United States Code is not intended as a blanket bar to former employees from dealing with the Government after separation. Rather, it represents a carefully crafted balance between preventing improper peddling of influence in the government by former government officials on the one hand, and permitting the continued availability to the government of the experience and training of former government officials. In a dynamic, forwarding leaning agency such as DHS, with a mission to protect the homeland, it is essential that the agency attract top notch people who are facile and knowledgeable about innovative technology. The DHS mission requires that these leaders in the fields populate the whole of DHS Headquarters and its components.

The statute is composite of a series of very fact specific prohibitions based on conclusions of improper over-reaching as determined though the lens of that balancing. Congress recognized the potential subsection 207(c) has to unduly restrict appropriate post-Government-service interaction by former employees with the government by carving out exceptions to it, i.e., subsection 207(c)(2)(B)(in the cases of special government employees), subsection 207(c)(2)(C)(in cases of difficult-to-fill positions), subsection 207(h)(in cases of elements of an agency where there exists "no potential for use of undue influence or unfair advantage based on past Government service"), and subsection 207(j)(Exceptions).

The recommendations that DHS made to the Director, Office of Government Ethics, in December 2003, were based on the following:

—OGE criteria for making such recommendations;
—how the Department was structured and operating;
—how the legacy agencies had treated the organizational elements previously; and
—how subsection 207(c) is applied generally through the Executive Branch.

Several features of the Department were clear for the purposes of these recommendations. United States Secret Service, the United State Coast Guard, the Transportation Security Agency, and the Federal Law Enforcement Training Center were focused on discrete independent missions of the Department, most statutorily so, and had extensive independent administrative structures. The three directorates, Science and Technology, Information Analysis and Infrastructure Protection, and Emergency Preparedness and Response, posed a more nuanced picture, but presented the same distinct, self-contained mission focuses.

Equally clear in the opposite direction was that the significance of the missions entrusted to the Border and Transportation Security Directorate and its subordinate elements and the extensive vertical and horizontal interaction between them made them so inter-related and inter-dependent as to foreclose designating them as separate.

Given those conclusions and comparing how other agencies treated their components, we recommended the designation of those seven components as separate for the purposes of the 1-year cooling-off period.

Question. How is this change beneficial to the Department, the U.S. taxpayers, and our national security?

Answer. The Department's exercise of this statute greatly enhances national security, benefits the taxpayers of the United States, and is invaluable in the accomplishment of the Department's mission. Detection of threats by passage of people and cargo into the United States by air, sea, or land is dependent upon innovative human and technological systems that are used by components throughout the Department. These systems were developed by career and non-career Federal employees working as a team. The career employees contribute their expertise and experience in government operations and the non-careerist often contribute their expertise and experience in technology developed in the private sector. It is a proven successful synergy, not quite perfect, but the best in the world.

Our nation's security and the taxpayer will be the ultimate losers if the country's professionals and leaders are kept from joining Federal agencies initially or, upon return to the private sector, are precluded from bringing their skills and experience to bear on these important issues because of a failure to appropriately tailor the post-Government-service restriction. The departing leaders take with them an understanding of the threat, what is needed to combat the threat, and how the Department is working to counter the threat. The threat is not stagnant, and it is counterproductive to overly restrict the work of those who are among the most able to ensure close cooperation and understanding between the Federal and non Federal entities to make our country safe.

We believe that the combination of the relaxation of the restriction imposed by section 207(c) granted by the designation of separate components and the existence of the additional restriction applicable to very senior personnel, the inapplicability of separate component designation to our former employees who were paid pursuant to the Executive Schedule, and the application of subsection 207(d), we have achieved the balance that was desired by the drafters of section 207. Of course, we must certify annually to the Director, United States Office of Government Ethics, that our designations remain appropriate.

DHS HEADQUARTERS

Question. In addition to the $25 million GSA is requesting to locate CG headquarters at St. Elizabeth's campus in Anacostia, there is a $13 million request for "St. Elizabeths West Campus Infrastructure". The West Campus alone has 182 acres and includes 61 buildings. The justification says "the site is aptly suited to provide a high security campus for Federal agencies."

What are the Department's plans for the St. Elizabeth site?

Answer. The Department's plans for the St. Elizabeth site are to ensure that the Coast Guard headquarters is properly planned and executed to provide additional expansion capability should the need arise for additional occupancy.

Question. How are these plans related to the current efforts to outfit the Nebraska Avenue complex?

Answer. The requirements for adjacency and mission needs being established at the NAC would be utilized should the opportunity for expansion be available at the St. Elizabeth site.

AVOIDING FUTURE FUND LAPSES

Question. Why did the Department Management account allow $9.3 million to lapse at the end of fiscal year 2004 and what specific systems have been put in place to make sure that this does not happen again?

Answer. The Department did not intentionally allow funding to lapse in fiscal year 2004. The fiscal year 2004 unobligated balance for the Departmental Management account was due primarily to slower than anticipated hiring, resulting in personnel lapse. In fiscal year 2004, the infrastructure and organization to manage budget execution for Departmental Management was not fully developed. The transition to a new accounting system and financial services provider in fiscal year 2004 created additional challenges and complexities, along with a learning curve, which made it difficult for financial managers to track spending during the year. In fiscal year 2005, we now have more staff and contractors onboard to perform budget execution activities for the Departmental Management account and can provide more useful data to managers to manage their budgets more efficiently and effectively.

Question. Do you plan to seek authority to reprogram the lapsed funds?

Answer. The Department submitted a request as part of the ICE reprogramming package to use the lapse authority under Section 504 to transfer $2.8 million from fiscal year 2004 lapsed funding from the Departmental Management account to ICE for its funding shortfall. This reprogramming request was overtaken by the fiscal year 2005 Emergency Supplemental Appropriations Act for Defense, the Global War on Terrorism and Tsunami Relief, H.R. 1268 recent Supplemental that was passed that rescinded a total of $3.8 million from Departmental Management that was proposed in the ICE programming, including the $2.8 million from the fiscal year 2004 lapsed monies.

CLASSIFIED VS. SENSITIVE INFORMATION

Question. Late last year there were articles in various papers, including The Washington Post, regarding how the Department handles information it determines to be "sensitive" versus actually "classified" material. It has required Federal Government employees, including congressional staff with "Top Secret" clearances, to sign confidentiality documents demanding that these previously cleared personnel

not reveal information that, technically, is not "classified". Most recently, on December 13, 2004, the Heritage Foundation released a report entitled, "DHS 2.0: Rethinking the Department of Homeland Security". One of its conclusions calls for the Department to develop a "consistent policy and legislation that encourages the sharing of unclassified but security-relevant information between the private sector and the government." This might also include the dropping or reconsideration of the documents security classification known as "Sensitive Security Information."

What public law created the classification known as "Sensitive Security Information"?

Answer. Following the terrorist attacks on the United States on September 11, 2001, Congress passed the Aviation and Transportation Security Act (ATSA), Public Law 107–71 (November 19, 2001), which established the Transportation Security Administration (TSA). ATSA transferred the responsibility for civil aviation security from the Federal Aviation Administration (FAA) to TSA. Among the statutory authorities previously administered by FAA that ATSA transferred to TSA's purview was the authority in 49 U.S.C. § 40119, governing the protection of certain information related to transportation security.

On February 22, 2002, TSA published a final rule transferring the bulk of FAA's aviation security regulations to TSA, including FAA's SSI regulation, which now is codified at 49 CFR Part 1520.

In addition, on November 25, 2002, the President signed into law the Homeland Security Act of 2002 (HSA), Public Law 107–296, which transferred TSA to the newly established DHS. In connection with this transfer, the HSA transferred TSA's SSI authority under 49 U.S.C. § 40119 to 49 U.S.C. § 114(s), and amended section 40119 to vest similar SSI authority in the Secretary of DOT. [See Section 1601 of the HSA.]

It should also be noted that Sensitive Security Information (SSI) is not a classification, and information designated as SSI is not considered as classified national security information.

Question. Is the Department, as part of your overall review of its operations, actively considering the Heritage Foundation recommendations on protecting sensitive information? If not, why not?

Answer. Yes. The Department has carefully reviewed a number of recommendations and proposals regarding information sharing, and it is working to develop and establish a consistent prudent strategy on the subject. The guiding principle must balance the need to share information with appropriate individuals, while still protecting the sensitive nature of the underlying information.

CONTRACTING OUT REPORT

Question. The fiscal year 2004 Appropriation Omnibus (H.R. 2673) Division F—Departments of Transportation and Treasury, and Independent Agencies, Title VI Section 647(b), contained the following reporting requirement: "Not later than 120 days following the enactment of this Act and not later than December 31 of each year thereafter, the head of each executive agency shall submit to Congress a report on the competitive sourcing activities on the list required under the Federal Activities Inventory Reform Act of 1998 (Public Law 105–270; 31 U.S.C. 501 note) that were performed for such executive agency during the previous fiscal year by Federal Government sources.

The Committee received this report on February 3, 2005. The report states that two public-private competitions, which were started in September of 2004, are scheduled for completion in fiscal year 2005. In addition, the report states that additional competitions are scheduled to be held in fiscal year 2005 which will involve up to 1,397 FTE.

Please provide the Committee an updated report containing the most recent fiscal year 2005 information as well as any plans for public-private competitions in fiscal year 2006.

Answer. In fiscal year 2005, DHS is currently completing the competitions involving 357 FTE. This includes competitions being conducted at the U.S. Coast Guard (USCG), CBP, and the FLETC. DHS is currently reviewing proposals for the completion of competitions in fiscal year 2006.

The DHS's annual Reports to Congress, as required by Section 647(b) of Division F of the Consolidated Appropriations Act, fiscal year 2004 (Public Law 108–199) are available on our web-site at: http://www.dhs.gov/dhspublic/display?theme=37&content=3933

Question. For fiscal year 2004 (actual), fiscal year 2005 (estimate), and fiscal year 2006 (request), how many positions in the Department (broken down by agency) were competed and how much did the competitions cost.

Answer. In fiscal year 2004, DHS completed three public-private competitions, in accordance with the OMB Circular A–76, involving 144 FTE at the USCG. Two DHS competitions that were scheduled for completion in fiscal year 2004 were cancelled in fiscal year 2004:

—The USCG's competition of its military travel support function (36 FTE) was cancelled due to the development of E-Travel technologies that will obviate the current approach to this service requirement;

—The Citizenship and Immigration Service (CIS) competition of its Immigration Information Officer (IIO) function (1,350 FTE) was cancelled to give more time and resources to the elimination of immigration service backlogs and, as a matter of law. DHS announced two ICE competitions for completion in fiscal year 2005. These competitions involved 97 FTE, but were also cancelled due to funding shortages.

Savings generated by the three completed fiscal year 2004 USCG competitions are estimated at $12.3 million over a 5 year period. All three competitions were retained in-house. The incremental cost of conducting these USCG studies is estimated at $1.3 million and reflects the costs incurred in gearing up the competition program in the USCG. In addition, four FTE are associated with DHS' fiscal year 2004 fixed costs—spread across the agency—and are estimated at $450,000 per year. The DHS fixed program cost estimate includes dedicated resources to provide central policy, planning, and implementation oversight, yet excludes annual FAIR Act inventory costs. The estimated one-time DHS cost of conducting the fiscal year 2005 competitions involving 356 FTE is $1.9 million, with expected annual savings in excess of $5 million. The estimated one-time cost of conducting the fiscal year 2006 competitions is not known, as we have not yet finalized those plans.

Question. How many positions were subsequently contracted out as a result of the competition?

Answer. While there have been significant efficiency and quality of service gains on the part of the government as a result of engaging in the fiscal year 2004 and fiscal year 2005 competitions, to date no positions have been converted to contract performance.

DETAILEES TO THE WHITE HOUSE

Question. How many DHS employees (including the component agencies) are currently detailed to the White House (including all Executive Office of the President agencies)? Provide the committee a list containing the originating agency; the office they are detailed to; salary grade/step; length of detail (including beginning and end dates); purpose of the detail; and indicate if the agency is reimbursed.

Answer.

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
NSC	DHS/IAIP	GS 12–01 ($62,886)	3/20/2004	12/30/2005	Communications and Media Relations. Was part of GSA technology office that was absorbed by DHS in early 2003.	N
NSC	DHS/USCG	MILITARY	6/14/2004	6/13/2006	White House Situation Room Duty Officer	N
NSC	DHS/USCG	MILITARY	6/21/2004	6/20/2005	Counternarcotics	N
NSC	DHS/USCG	MILITARY	10/6/2003	6/10/2005	White House Situation Room Duty Officer	N
NSC	USSS	GS 14–02 ($91,315)	4/18/2005	4/17/2006	Combating Terrorism	N
ONDCP	U.S. Coast Guard	MILITARY	7/15/2004	7/15/2005	Office of Supply Reduction	N
WHO	DHS/TSA	K–00 ($111,038)	5/21/2004	9/30/2005	Support the WHO mission	N
WHO	DHS		7/24/2004	1/19/2006	Support the WHO mission	N
WHO	DHS/USSS	GS 14–04 ($97,206)	6/22/2004	9/30/2005	Support the WHO mission	N
WHO	U.S. Coast Guard	MILITARY	9/22/2004	1/19/2006	Support the WHO mission	N
OVP	U.S. Coast Guard	MILITARY	5/17/2005	7/15/2007	Military Aide to the Vice President	N
OVP	U.S. Coast Guard	MILITARY	6/16/2003	7/1/2005	Special Advisor, Homeland Security	N
OVP	U.S. Coast Guard	MILITARY	4/22/2003	6/29/2005	Military Aide to the Vice President	N

DETAILEES TO THE DEPARTMENT

Question. How many employees of DHS component agencies are currently detailed to the Department? Provide the committee a list containing the originating agency; the office they are detailed to; salary grade/step; length of detail (including beginning and end dates); purpose of the detail; and indicate if this agency is reimbursed.

Answer. The table below provides the requested data, which is a snapshot of detailees on-board as of March 31, 2005. This data submission was done in April 2005 and projected end dates that could have ended by the time this report was submitted.

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
USM/CIO	BTS	$117,809	6/1/2004	6/1/2005	DHS Infrastructure trans support	N
BTS	CBP	$149,200	7/27/2004	7/27/2005	BTS	N
BTS	CBP	$121,274	9/2/2003	9/2/2005	Cargo/Trade Policy	N
BTS	CBP	$117,809	9/7/2004	9/6/2005	Border Patrol Liaison	N
BTS	CBP	$117,809	2/23/2003	(1)	Counternarcotics Projects	N
BTS	CBP	$100,152	7/27/2004	7/27/2005	CIO Assistant	N
BTS	CBP	$94,260	12/6/2004	12/7/2005	Agency Liaison Officer	N
FLETC	CBP	$81,638	10/7/2002	(1)	Instructor	N
FLETC	CBP	$81,638	5/15/1995	(1)	Instructor	N
FLETC	CBP	$81,638	9/2/2003	9/2/2006	Instructor	N
FLETC	CBP	$68,651	5/1/2004	5/1/2007	Instructor	N
FLETC	CBP	$81,638	2/18/1998		Instructor	N
FLETC	CBP	$68,651	10/1/2002	(1)	Instructor	N
FLETC	CBP	$81,638	2/16/1993		Instructor	N
FLETC	CBP	$68,651	5/16/2004	5/16/2007	Instructor	N
FLETC	CBP	$81,638	11/19/2001	(1)	Instructor	N
FLETC	CBP	$81,638	8/13/1998		Instructor	N
FLETC	CBP	$68,651	10/27/2003	10/27/2008	Instructor	N
FLETC	CBP	$68,651	(2)	(1)	Instructor	N
FLETC	CBP	$81,638	11/6/1990		Instructor	N
FLETC	CBP	$81,638	(2)	(1)	Instructor	N
FLETC	CBP	$81,638	9/25/2000		Instructor	N
FLETC	CBP	$81,638	3/22/2004	3/22/2007	Instructor	N
FLETC	CBP	$81,638	12/23/2000		Instructor	N
FLETC	CBP	$81,638	6/1/1998	(1)	Instructor	N
FLETC	CBP	$81,638	9/29/1997		Instructor	N
FLETC	CBP	$81,638	1/25/1993	(1)	Instructor	N
FLETC	CBP	$68,651	2/24/2004	(1)	Instructor	N
FLETC	CBP	$81,638	7/30/1997	(1)	Instructor	N
FLETC	CBP	$81,638	8/27/2001	8/27/2006	Instructor	N
FLETC	CBP	$57,280	4/15/2002	4/15/2007	Instructor	N
FLETC	CBP	$68,651	7/14/2003	(1)	Instructor	N
IAIP	CBP	$131,671	10/1/2004	(1)	HSOC	N
IAIP	CBP	$91,315	1/10/2005	7/10/2005	Terrorist Screening Ctr	N
IAIP	CBP	$69,173	11/28/2004	5/17/2005	HSOC	N
IAIP	CBP	$73,364	11/29/2004	5/17/2005	HSOC	N
IAIP	CBP	$75,460	11/29/2004	5/17/2005	HSOC	N
IAIP	CBP	$62,886	11/17/2003	5/31/2005	Support to IAIP Terrorist Screening Center	N

IAIP	CBP	$77,274	9/12/2003	(1)	HSOC	N
IAIP	CBP	$69,173	12/12/2004	6/14/2005	HSOC	N
IAIP	CBP	$77,274	3/20/2005	3/20/2006	COMSEC	N
ICE	CBP	$52,468	3/21/2005	3/21/2006	Visa Security Program	N
ICE	CBP	$124,274	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$43,724	11/1/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$61,213	10/23/2004	3/31/2005	Visa Security Unit	N
ICE	CBP	$91,315	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$97,213	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$91,315	9/20/2004	6/1/2005	Visa Security Unit	N
ICE	CBP	$68,209	11/17/2004	4/29/2005	Visa Security Unit	N
ICE	CBP	$117,809	12/7/2004	TBA	Assist ICE HR Officer	N
OIA	CBP	$62,886	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OIA	CBP	$57,715	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OIA	CBP	$64,981	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OPA	CBP	$128,205	1/26/2004	(1)	Public Affairs	N
USCG	CBP	$77,274	8/4/2003	(1)	Support to USCG	N
USM/CFO	CBP	$114,344	1/1/2004	(1)	OCFO	N
USM/CFO	CBP	$103,947	10/20/2003	10/19/2005	Support eMerge project	N
USM/CFO	CBP	$106,044	10/1/2003	10/1/2005	Support eMerge project	N
USM/CHCO	CBP	$100,152	4/28/2004	(1)	New HR system: communications team	N
USM/CIO	CBP	$100,152	5/1/2004	5/1/2005	Infrastructure Transformation Office	N
USM/CIO	CBP	$117,344	11/10/2003	6/30/2005	Program manager—HSDN	N
USM/CIO	CBP	$149,200	10/6/2004	7/31/2005	CIO	N
USM/CIO	CBP	$43,365	11/9/2004	9/15/2005	CIO support	N
S&T	CG	$84,751	6/30/2004	6/30/2007	Providing technical expertise to S&T	Y
USM/CIO	CIS	$89,736	3/1/2003	(1)	Support DHS' Infrastructure Transformation Office	N
USM/CIO	CIS					N
S&T	DHS	$100,152	2/22/2005	6/21/2005	Providing admin support to HHS	Y
S&T	DHS	$59,464	11/1/2004	6/30/2005	Providing admin support to HHS	Y
S&T	DHS	$117,809	1/14/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/NAC	$100,152	1/31/2005	(1)	Support DNDO Transition Team for Stand-up	N
NCR	DHS/ODP	$135,136	Unknown	(1)	Nat Cap Reg mission support	N
OSLGC	DHS/ODP	$84,751	2/7/2005	8/6/2005	Support to OSLGCP	N
OSLGC	DHS/ODP	$100,152	2/7/2005	8/6/2005	Support to OSLGCP	N
S&T	DHS/ODP	$117,809	2/7/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$117,809	1/10/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,152	1/10/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,600	1/10/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,600	3/1/2005	(1)	Support DNDO Transition Team for Stand-up	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
FLETC	Federal Air Marshal Service	$96,474	2/7/2005	2/7/2006	On the job Training	N
FLETC	Federal Protective Service	$68,651	10/1/2003	10/1/2006	Instructor	N
FLETC	Federal Protective Service	$68,651	10/20/2003	10/20/2006	Instructor	N
FLETC	Federal Protective Service	$68,651	11/1/2003	11/1/2006	Instructor	N
IAIP	FEMA	$114,882			Support to IAIP mission	N
IAIP	FEMA	$135,136			Support to IAIP mission	N
OSLGC	FEMA	13/3	1/27/2003	TBD	Support to State and Local Coordination and Outreach	N
USM/CFO	FEMA	$100,152	8/1/2004	5/1/2005	Support GAO/IG Liaison Office	N
USM/CHCO	FEMA	$84,751	5/3/2004	1/31/2005	Design of new DHS Personnel HR management system	N
ODP	FEMA/Region III	$82,259	7/11/2004	(1)	Implementation of ODP Program into DHS—move from FEMA Citizen Corp Assistance.	
BTS	FLETC	$100,152	8/1/2003	8/1/2005	FLETC Liaison	N
USM/CFO	FLETC	$100,152	2/1/2005	2/1/2006	Support eMerge project	N
BTS	ICE	$100,152	4/12/2004	4/12/2006	Immigration Policy Advisor	N
BTS	ICE	$117,809	3/10/2003	(1)	Immigration Policy Advisor	N
BTS	ICE	$49,145	11/30/2004	(1)	Protective detail	N
BTS	ICE	$44,495	10/22/2003	(1)	Scheduling Support for Under Secretary	N
BTS	ICE	$69,000	3/14/2005	9/15/2005	FAMS Liaison	N
BTS	ICE	$84,751	9/2/2003	(1)	ICE Liaison	N
BTS	ICE	$71,269	6/29/2003	(1)	Advance Work for Under Secretary	Y
BTS	ICE	$49,145	2/27/2005	6/25/2005	Protective detail	N
BTS	ICE	$100,152	8/3/2004	8/3/2005	ICE Liaison	N
BTS	ICE	$71,269	6/29/2003	(1)	Advance Work for Under Secretary	Y
BTS	ICE	$100,152	7/1/2004	7/1/2005	Setting up office w/detailees from bureaus (Office of Screening and Coordination).	
CBP	ICE	$100,152	1/1/2005	(1)	Liaison to NTC	N
CBP	ICE	$84,751	12/15/2003	(1)	ICE Liaison	N
CIS	ICE	$59,464	4/1/2004	(1)	Long-term detail to provide paralegal services	N
DHS	ICE	$100,152	7/1/2004	7/1/2005	DHS/CFO	N
DHS	ICE	$117,809	9/1/2003	9/1/2006	Rep to Interpol as Dep Dir for OIA	
FEMA	ICE	$49,145	8/1/2004	(1)	Protective detail	N
FLETC	ICE	$81,638	9/19/2004	9/19/2009	Instructor	N
FLETC	ICE	$81,638	1/15/2003	(1)	Instructor	N
FLETC	ICE	$81,638	5/20/1996	(1)	Instructor	N
FLETC	ICE	$81,638	3/1/1988	(1)	Instructor	N
FLETC	ICE	$81,638	3/1/2001	(1)	Instructor	N
FLETC	ICE	$81,638	9/1/2004	9/1/2007	Instructor	N

FLETC	ICE	$81,638	9/1/2003	9/1/2006	Instructor	N
FLETC	ICE	$81,638	3/10/2002	3/1/2007	Instructor	N
FLETC	ICE	$81,638	1/23/2003	12/6/2006	Instructor	N
FLETC	ICE	$81,638	11/4/2001	11/4/2006	Instructor	N
FLETC	ICE	$81,638	9/8/2003	9/7/2006	Instructor	N
FTTTF	ICE	$100,152	1/1/2003	(1)	Liaison; NSEERS Tracking	N
IAIP	ICE	$100,152	7/1/2003	(1)	Support to IAIP mission	N
IAIP	ICE	$100,152	1/1/2004	(1)	Interpol Liaison	N
IAIP	ICE	$100,152	1/12/2004	(1)	Serve as ICE rep and subject matter expert	
IAIP	ICE	$100,152	11/1/2003	(1)	Support to IAIP mission	N
IAIP	ICE	$71,269	8/24/2003	(1)	Support to IAIP mission	N
IAIP	ICE	$71,269	8/24/2003	(1)	ICE/BTS Liaison	N
IAIP	ICE	$100,152	1/1/2004	(1)	Interpol Liaison	N
IAIP	ICE	$100,152	1/11/2004	(1)	Support to IAIP mission	N
IAIP	ICE	$84,751	1/1/2004	(1)	Support to IAIP mission	N
IAIP	ICE	$100,152	6/1/2004	6/1/2006	ICE Liaison	Y
IAIP	ICE	$100,152	Jan. 2000	(1)	Support to IAIP mission—DOS Liaison	N
IAIP	ICE	$69,000	7/4/2005	(1)	Intelligence Sharing HSOC	N
IAIP	ICE	$100,152	3/1/2003	3/1/2006	Support to IAIP mission—DHS Liaison to FBI	N
IAIP	ICE	$117,809	2/19/2002	(1)	Support to IAIP mission—HSOC	Y
IAIP	ICE	$100,152	11/1/2003	(1)	Support to IAIP mission	N
IAIP	ICE	$84,751	1/1/2003	(1)	Support to IAIP mission—HSOC desk officer	N
IAIP	ICE	$100,152	3/1/2003	(1)	Support to IAIP mission	N
ICE	ICE	$84,751	3/1/2002	(1)	ICE Liaison	N
OLA	ICE	$84,751	1/1/2004	(1)	Leg Affairs liaison to Immigration	N
OPA	ICE	$100,152	1/1/2003	(1)	Support to Public Affairs	N
USCG	ICE	$100,152	8/1/2004	(1)	Coast Guard Liaison	N
USM/CIO	ICE		7/12/04	7/8/05	Provide on-site geospatial technical support	N
USM/CIO	ICE	$100,152	12/1/2003	(1)	Program management and acquisition support	N
USM/CIO	ICE	$117,809	10/1/2003	(1)	Director, Infrastructure Transformation Office	N
BTS	TSA	$56,600	6/7/2004	6/7/2005	Provides admin support services to the AA at BTS	N
BTS	TSA	SW–02	2/1/2004	(1)	BTS Deputy Chief of Staff	N
BTS	TSA	$69,000	2/17/2004	(1)	Transportation Security Policy Advisor	N
BTS	TSA	$84,150	12/13/2004	12/13/2005	TSA Liaison	N
BTS	TSA	$84,150	12/31/2004	12/13/2005	Serves as TSA liaison to BTS	N
BTS	TSA	$69,000	7/26/2004	4/2/2005	Provides legislative policy assistance to AA	N
BTS	TSA	$38,900	2/28/2005	10/4/2005	Correspondence Analyst	N
BTS	TSA	$100,600	8/11/2003	8/11/2006	International Affairs	N
BTS	TSA	$100,600	3/23/2003	(1)	National Counter Terrorist Center on SpecialProject	N
BTS	TSA	$46,400	2/2/2004	(1)	Speech Writer	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
BTS	TSA	$84,150	3/7/2005	(1)	Special Asst to Under Secretary	N
BTS	TSA	$100,600	9/26/2004	9/26/2005	Establishing the Office of Screening Coordination for DHS/BTS	N
DHS–OPL	TSA	$84,150	2/13/2005	6/13/2005	Serves as a special assistant for senior level officials TOPOFF3 Program	N
IAIP	TSA	$84,150	3/1/2003	(1)	Support to IAIP mission	N
IAIP	TSA	$69,000	10/1/2003	(1)	Support to IAIP mission	N
ICE	TSA	$100,600	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$100,600	1/10/2005	4/9/2005	Task force to review ICE budget	N
ICE	TSA	$100,600	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$84,150	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$100,600	1/10/2005	4/9/2005	Assisting with ICE budget audit	N
OGC	TSA	$84,150	8/8/2005	8/8/2007	Provide legal advice concerning border and transportation security issues especially as they involve TSA.	N
OPA	TSA	$84,150	3/3/2003	(1)	Public Affairs assisting on special project (requested by Dennis Murphy)	N
Security	TSA	$100,600	12/12/2004	4/2/2005	Requested for special project on security initiatives at the Chief Security Office.	N
USM	TSA	$120,250	12/26/2004	(1)	Acting Deputy Director Business Transformation office—Selected for DHS position, awaiting clearance through security process.	N
USM	TSA	$158,568	8/30/2004	9/30/2005	Acting Dir, Business Transformation Off	
USM/CFO	TSA	$100,152	10/1/2003	10/1/2005	Support eMerge project	N
USM/CIO	TSA	$149,200	4/3/2005	(1)	Support Solutions Engineering COE	Y
USM/CIO	TSA	$152,824	7/13/2003	4/1/2005	Acting Deputy CIO	Y
USM/CIO	TSA	$141,844	7/13/2003	(1)	DHS/BTS Integration	N
USM/CIO	TSA	$110,278	4/3/2005	9/30/2005	Information Technology	Y
USM/CIO	TSA	$145,482	10/27/2004	(1)	TSA representative to the Information Technology Officer	N
USM/CIO	TSA	$138,093	4/3/2005	9/30/2005	Information Technology	Y
USM/CIO	TSA	$141,454	7/13/2003	(1)	INFRASTRUCTURE program support	Y
IAIP	USCG	$136,490	9/19/2003	9/19/2005	HSC Watch Augmentation	N
OGC	USCG	$82,937	3/1/2005	3/1/2007	Assist with international issues and with Team Telecom/CFIUS legal issues	N
Security	USCG	$56,128	12/1/2004	Ongoing	State and Local Investigations	Y
Security	USCG	$82,937	12/1/2004	(3)	State and Local Investigations	Y
Security	USCG	$71,269	12/1/2004	(3)	State and Local Investigations	Y
Security	USCG	$74,560	12/1/2004	(3)	State and Local Investigations	Y
USM/CFO	USCG	$101,613	8/1/2004	8/1/2005	Support Budget Office	N
USM/CFO	USCG	$82,937	1/5/2005	4/1/2005	ICE Tiger Team	N
USM/CIO	USCG	$156,886		(1)	Support DHS' Infrastructure Transformation Office	Y
IAIP	USCIS	$74,782	3/21/2005	5/21/2005	To assist in setting up DHS' Operations Center	N
IAIP	USCIS	$74,782	3/21/2005	5/21/2005	To assist in setting up DHS' Information Analysis Section	N

ICE	USCIS	$87,244	1/3/2005	(1)	To assist ICE in prosecuting Operation Jakarta Asylum Applications—detail lasts until this case goes to trial.	N
ICE	USCIS	$75,460	3/7/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraudinvestigation).	N
ICE	USCIS	$41,361	3/7/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
ICE	USCIS	$64,981	3/14/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
BTS	USSS	$97,206	2/21/2004	8/21/2005	Border & Transp. Security	N
DHS/IAIP	USSS	$91,315	6/1/2004	12/1/2005	Investigations	N
FEMA	USSS	$91,315	10/17/2004	4/17/2005	DEST Program	N
FLETC	USSS	$68,651	8/1/2003	8/10/2008	Instructor	N
FLETC	USSS	$81,638	3/20/2005	3/20/2008	Instructor	N
FLETC	USSS	$68,651	1/1/2003	1/1/2006	Instructor	N
FLETC	USSS	$58,564	6/1/2000	6/1/2005	Instructor	N
FLETC	USSS	$81,638	2/1/2003	2/1/2006	Instructor	N
FLETC	USSS	$63,040	1/12/2004	1/12/2007	Instructor	N
FLETC	USSS	$81,638	2/9/2004	2/9/2009	Instructor	N
FLETC	USSS	$81,638	10/6/2002	12/6/2005	Instructor	N
FLETC	USSS	$81,638	9/1/2003	9/1/2006	Instructor	N
FLETC	USSS	$81,638	9/1/2003	9/1/2005	Instructor	N
IAIP	USSS	$84,751	10/19/2003	5/29/2005	Nat. CounterTerrorism Ctr	N
IAIP	USSS	UND—LT	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$77,274	3/13/2005	6/11/2005	HS Operations Center	N
IAIP	USSS	$100,152	1/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$114,344	5/7/2004	7/10/2005	Protective Research (IAIP)	N
IAIP	USSS	$40,179	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	UND—Off	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	11/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	5/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$97,206	2/8/2004	8/8/2005	Protective Research (IAIP)	N
IAIP	USSS	$103,947	9/1/2004	9/1/2005	Investigations	N
IAIP	USSS	$87,244	2/27/2005	5/28/2005	HS Operations Center	N
IAIP	USSS	$84,751	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$110,878	6/1/2003	(3)	Support to IAIP mission—Investigations	Y
IAIP	USSS	$36,157	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	12/1/2003	(3)	Support to IAIP mission	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
IAIP	USSS	$74,782	3/6/2005	6/4/2005	HS Operations Center	N
IAIP	USSS	$79,766	5/1/2004	5/1/2005	Investigations	N
IAIP	USSS	$100,152	10/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	1/1/2003	(3)	Support to IAIP mission	N
OSLGC	USSS	$88,000	10/3/2004	4/3/2005	Law Enforcement Liaison	N
S&T	USSS	$100,152	2/1/2003	(1)	Providing technical expertise to S&T	N
S&T	USSS	$97,206	1/1/2003	(1)	Providing technical expertise to S&T—Protective Research (INT)	N
Security	USSS	$97,206	7/21/2003	7/21/2005	Counter Intelligence	N
Security	USSS	$88,000	2/1/2003	(1)	Provides physical security to DHS facilities	N
Security	USSS	$94,000	2/23/2003	8/23/2005	Phy. Sec & Access Ctrl	N
USM/CHCO	USSS	$91,315	3/10/2004	4/1/2005	New HR system: pay and performance team	N
USM/CHCO	USSS	$82,259	2/1/2005	5/16/2005	Hiring and transition response team	N
USM/CIO	BTS	$117,809	6/1/2004	6/1/2005	DHS Infrastructure trans support	N
BTS	CBP	$149,200	7/27/2004	7/27/2005	BTS	N
BTS	CBP	$121,274	9/2/2003	9/2/2005	Cargo/Trade Policy	N
BTS	CBP	$117,809	9/7/2004	9/6/2005	Border Patrol Liaison	N
BTS	CBP	$117,809	2/23/2003	(1)	Counternarcotics Projects	N
BTS	CBP	$100,152	7/27/2004	7/27/2005	CIO Assistant	N
BTS	CBP	$94,260	12/6/2004	12/7/2005	Agency Liaison Officer	N
FLETC	CBP	$81,638	10/7/2002	(1)	Instructor	N
FLETC	CBP	$81,638	5/15/1995	(1)	Instructor	N
FLETC	CBP	$81,638	9/2/2003	9/2/2006	Instructor	N
FLETC	CBP	$68,651	5/1/2004	5/1/2007	Instructor	N
FLETC	CBP	$81,638	2/18/1998	(1)	Instructor	N
FLETC	CBP	$68,651	10/1/2002	(1)	Instructor	N
FLETC	CBP	$81,638	2/16/1993	(1)	Instructor	N
FLETC	CBP	$68,651	5/16/2004	5/16/2007	Instructor	N
FLETC	CBP	$81,638	11/19/2001	(1)	Instructor	N
FLETC	CBP	$81,638	8/13/1998	(1)	Instructor	N
FLETC	CBP	$68,651	10/27/2003	10/27/2008	Instructor	N
FLETC	CBP	$68,651	(2)	(1)	Instructor	N
FLETC	CBP	$81,638	11/6/1990	(1)	Instructor	N
FLETC	CBP	$81,638	(2)	(1)	Instructor	N
FLETC	CBP	$81,638	9/25/2000	(1)	Instructor	N
FLETC	CBP	$81,638	3/22/2004	3/22/2007	Instructor	N
FLETC	CBP	$81,638	12/23/2000	(1)	Instructor	N
FLETC	CBP	$81,638	6/1/1998	(1)	Instructor	N

FLETC	CBP	$81,638	9/29/1997	(1)	Instructor	N
FLETC	CBP	$81,638	1/25/1993	(1)	Instructor	N
FLETC	CBP	$68,651	2/24/2004	(1)	Instructor	N
FLETC	CBP	$81,638	7/30/1997	(1)	Instructor	N
FLETC	CBP	$81,638	8/27/2001	8/27/2006	Instructor	N
FLETC	CBP	$57,280	4/15/2002	4/15/2007	Instructor	N
FLETC	CBP	$68,651	7/14/2003	(1)	Instructor	N
IAIP	CBP	$131,671	10/1/2004	(1)	HSOC	N
IAIP	CBP	$91,315	1/10/2005	7/10/2005	Terrorist Screening Ctr	N
IAIP	CBP	$69,173	11/28/2004	5/17/2005	HSOC	N
IAIP	CBP	$73,364	11/29/2004	5/17/2005	HSOC	N
IAIP	CBP	$75,460	11/29/2004	5/17/2005	HSOC	N
IAIP	CBP	$62,886	11/17/2003	5/31/2005	Support to IAIP Terrorist Screening Center	N
IAIP	CBP	$77,274	9/12/2003	(1)	HSOC	N
IAIP	CBP	$69,173	12/12/2004	6/14/2005	HSOC	N
IAIP	CBP	$77,274	3/20/2005	3/20/2006	COMSEC	N
ICE	CBP	$52,468	3/21/2005	3/21/2006	Visa Security Program	N
ICE	CBP	$124,274	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$43,724	11/1/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$91,315	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$97,213	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$91,315	9/20/2004	6/1/2005	Visa Security Unit	N
ICE	CBP	$68,209	11/17/2004	4/29/2005	Visa Security Unit	N
ICE	CBP	$117,809	12/7/2004	TBD	Assist ICE HR Officer	N
OIA	CBP	$62,886	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OIA	CBP	$57,715	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OIA	CBP	$64,981	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OPA	CBP	$128,205	1/26/2004	(1)	Public Affairs	N
USCG	CBP	$77,274	8/4/2003	(1)	Support to USCG	N
USM/CFO	CBP	$114,344	1/1/2004	(1)	OCFO	N
USM/CFO	CBP	$103,947	10/20/2003	10/19/2005	Support eMerge project	N
USM/CFO	CBP	$106,044	10/1/2003	10/1/2005	Support eMerge project	N
USM/CHCO	CBP	$100,152	4/28/2004	(1)	New HR system: communications team	N
USM/CIO	CBP	$100,152	5/1/2004	5/1/2005	Infrastructure Transformation Office	N
USM/CIO	CBP	$117,344	11/10/2003	6/30/2005	Program manager—HSDN	N
USM/CIO	CBP	$149,200	10/6/2004	7/31/2005	CIO	N
USM/CIO	CBP	$43,365	11/9/2004	9/15/2005	CIO support	N
S&T	CG	$84,751	6/30/2004	6/30/2007	Providing technical expertise to S&T	Y
OGC	CIS	$110,878	9/1/2003	9/1/2006	Provide substantive immigration expertise to DHS OGC, focusing on issues relating to immigration benefits and related USCIS issues.	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
USM/CIO	CIS	$89,736	3/1/2003	(1)	Support DHS' Infrastructure Transformation Office	N
USM/CIO	CIS					N
S&T	DHS	$100,152	2/22/2005	6/21/2005	Providing admin support to HHS	Y
S&T	DHS	$59,464	11/1/2004	6/30/2005	Providing admin support to HHS	Y
S&T	DHS	$117,809	1/14/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/NAC	$100,152	1/31/2005	(1)	Support DNDO Transition Team for Stand-up	N
OSLGC	DHS/ODP	$84,751	2/7/2005	8/6/2005	Support to OSLGCP	N
OSLGC	DHS/ODP	$100,152	2/7/2005	8/6/2005	Support to OSLGCP	N
S&T	DHS/ODP	$117,809	2/7/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$117,809	1/10/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,152	1/10/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,600	1/10/2005	Indefinite	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,600	3/1/2005	Indefinite	Support DNDO Transition Team for Stand-up	N
FLETC	Federal Air Marshal Service	$96,474	2/7/2005	2/7/2006	On the job Training	N
FLETC	Federal Protective Service	$68,651	10/1/2003	10/1/2006	Instructor	N
FLETC	Federal Protective Service	$68,651	10/20/2003	10/20/2006	Instructor	N
FLETC	Federal Protective Service	$68,651	11/1/2003	11/1/2006	Instructor	N
OSLGC	FEMA	13/3	1/27/2003	TBD	Support to State and Local Coordination and Outreach	N
USM/CFO	FEMA	$100,152	8/1/2004	5/1/2005	Support GAO/IG Liaison Office	N
ODP	FEMA/Region III	$82,259	7/11/2004	Indefinite	Implementation of ODP Program into DHS—move from FEMA Citizen Corp Assistance.	N
BTS	FLETC	$100,152	8/1/2003	8/1/2005	FLETC Liaison	N
USM/CFO	FLETC	$100,152	2/1/2005	2/1/2006	Support eMerge project	N
BTS	ICE	$100,152	4/12/2004	4/12/2006	Immigration Policy Advisor	N
BTS	ICE	$117,809	3/10/2003	Indefinite	Immigration Policy Advisor	N
BTS	ICE	$49,145	11/30/2004	Indefinite	Protective detail	N
BTS	ICE	$44,495	10/22/2003	Indefinite	Scheduling Support for Under Secretary	N
BTS	ICE	$69,000	3/14/2005	9/15/2005	FAMS Liaison	N
BTS	ICE	$84,751	9/2/2003	Indefinite	ICE Liaison	N
BTS	ICE	$71,269	6/29/2003	Indefinite	Advance Work for Under Secretary	Y
BTS	ICE	$49,145	2/27/2005	6/25/2005	Protective detail	N
BTS	ICE	$100,152	8/3/2004	8/3/2005	ICE Liaison	N
BTS	ICE	$71,269	6/29/2003	Indefinite	Advance Work for Under Secretary	Y
BTS	ICE	$100,152	7/1/2004	7/1/2005	Setting up office w/ detailees from bureaus (Office of Screening and Coordination).	N
CBP	ICE	$100,152	1/1/2005	Indefinite	Liaison to NTC	N
CBP	ICE	$84,751	12/15/2003	Indefinite	ICE Liaison	N

CIS	ICE	$59,464	4/1/2004	Indefinite	Long-term detail to provide paralegal services	N
DHS	ICE	$100,152	7/1/2004	7/1/2005	DHS/CFO	N
DHS	ICE	$117,809	9/1/2003	9/1/2006	Rep to Interpol as Dep Dir for OIA	N
FEMA	ICE	$49,145	8/1/2004	Indefinite	Protective detail	N
FLETC	ICE	$81,638	9/19/2004	9/19/2009	Instructor	N
FLETC	ICE	$81,638	1/15/2003	Indefinite	Instructor	N
FLETC	ICE	$81,638	5/20/1996	Indefinite	Instructor	N
FLETC	ICE	$81,638	3/1/1988	Indefinite	Instructor	N
FLETC	ICE	$81,638	3/1/2001	Indefinite	Instructor	N
FLETC	ICE	$81,638	9/1/2004	9/1/2007	Instructor	N
FLETC	ICE	$81,638	9/1/2003	9/1/2006	Instructor	N
FLETC	ICE	$81,638	3/10/2002	3/1/2007	Instructor	N
FLETC	ICE	$81,638	1/23/2003	12/6/2006	Instructor	N
FLETC	ICE	$81,638	11/4/2001	11/4/2006	Instructor	N
FLETC	ICE	$81,638	9/8/2003	9/7/2006	Instructor	N
IAIP	ICE	$100,152	7/1/2003	Indefinite	Support to IAIP mission	N
IAIP	ICE	$100,152	1/1/2004	Indefinite	Interpol Liaison	N
IAIP	ICE	$100,152	1/12/2004	Indefinite	Serve as ICE rep and subject matter expert	N
IAIP	ICE	$100,152	11/1/2003	Indefinite	Support to IAIP mission	N
IAIP	ICE	$71,269	8/24/2003	Indefinite	Support to IAIP mission	N
IAIP	ICE	$71,269	8/24/2003	Indefinite	ICE/BTS Liaison	N
IAIP	ICE	$100,152	1/1/2004	Indefinite	Interpol Liaison	N
IAIP	ICE	$100,152	1/11/2004	Indefinite	Support to IAIP mission	N
IAIP	ICE	$84,751	1/1/2004	Indefinite	Support to IAIP mission	N
IAIP	ICE	$100,152	6/1/2004	6/1/2006	ICE Liaison	Y
IAIP	ICE	$100,152	Jan. 2000	Indefinite	Support to IAIP mission—DOS Liaison	N
IAIP	ICE	$69,000	7/4/2005	Indefinite	Intelligence Sharing HSOC	N
IAIP	ICE	$100,152	3/1/2003	3/1/2006	Support to IAIP mission—DHS Liaison to FBI	N
IAIP	ICE	$117,809	2/19/2002	Indefinite	Support to IAIP mission—HSOC	Y
IAIP	ICE	$100,152	11/1/2003	Indefinite	Support to IAIP mission	N
IAIP	ICE	$84,751	1/1/2003	Indefinite	Support to IAIP mission—HSOC desk officer	N
IAIP	ICE	$100,152	3/1/2003	Indefinite	Support to IAIP mission	N
ICE	ICE	$84,751	3/1/2002	Indefinite	ICE Liaison	N
OLA	ICE	$84,751	1/1/2004	Indefinite	Leg Affairs liaison to Immigration	N
OPA	ICE	$100,152	1/1/2003	Indefinite	Support to Public Affairs	N
USCG	ICE	$100,152	8/1/2004	Indefinite	Coast Guard Liaison	N
USM/CIO	ICE	.....	7/12/04	7/8/05	Provide on-site geospatial technical support	N
USM/CIO	ICE	$100,152	12/1/2003	Indefinite	Program management and acquisition support	N
USM/CIO	ICE	$117,809	10/1/2003	Indefinite	Director, Infrastructure Transformation Office	N
BTS	TSA	$56,600	6/7/2004	6/7/2005	Provides admin support services to the AA at BTS	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
BTS	TSA	SW–02	2/1/2004	Indefinite	BTS Deputy Chief of Staff	N
BTS	TSA	$69,000	2/17/2004	Indefinite	Transportation Security Policy Advisor	N
BTS	TSA	$84,150	12/13/2004	12/13/2005	TSA Liaison	N
BTS	TSA	$84,150	12/31/2004	12/13/2005	Serves as TSA liaison to BTS	N
BTS	TSA	$100,600	7/13/2003	1/22/2005	Operations Executive Assistant	N
BTS	TSA	$69,000	7/26/2004	4/2/2005	Provides legislative policy assistance to AA	N
BTS	TSA	$38,900	2/28/2005	10/4/2005	Correspondence Analyst	N
BTS	TSA	$100,600	8/11/2003	8/11/2006	International Affairs	N
BTS	TSA	$100,600	3/23/2003	Indefinite	National Counter Terrorist Center on special project	N
BTS	TSA	$46,400	2/2/2004	Indefinite	Speech Writer	N
BTS	TSA	$84,150	3/7/2005	Indefinite	Special Asst to Under Secretary	N
BTS	TSA	$100,600	9/26/2004	9/26/2005	Establishing the Office of Screening Coordination for DHS/BTS	N
DHS–OPL	TSA	$84,150	2/13/2005	6/13/2005	Serves as a special assistant for senior level officials TOPOFF3 Program	N
IAIP	TSA	$84,150	3/1/2003	Indefinite	Support to IAIP mission	N
IAIP	TSA	$69,000	10/1/2003	Indefinite	Support to IAIP mission	N
ICE	TSA	$100,600	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$100,600	1/10/2005	4/9/2005	Task force to review ICE budget	N
ICE	TSA	$100,600	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$84,150	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$100,600	1/10/2005	4/9/2005	Assisting with ICE budget audit	N
OGC	TSA	$84,150	8/8/2005	8/8/2007	Provide legal advice concerning border and transportation security issues especially as they involve TSA.	N
OPA	TSA	$84,150	3/3/2003	Indefinite	Public Affairs assisting on special project(requested by Dennis Murphy)	N
Security	TSA	$100,600	12/12/2004	4/2/2005	Requested for special project on security initiatives at the Chief Security Office.	N
USM	TSA	$120,250	12/26/2004	Indefinite	Acting Deputy Director Business Transformation office—Selected for DHS position, awaiting clearance through security process.	N
USM	TSA	$158,568	8/30/2004	9/30/2005	Acting Dir, Business Transformation Off	N
USM/CFO	TSA	$100,152	10/1/2003	10/1/2005	Support eMerge project	N
USM/CIO	TSA	$149,200	4/3/2005	Indefinite	Support Solutions Engineering COE	Y
USM/CIO	TSA	$152,824	7/13/2003	4/1/2005	Acting Deputy CIO	Y
USM/CIO	TSA	$141,844	7/13/2003	Indefinite	DHS/BTS Integration	N
USM/CIO	TSA	$110,278	4/3/2005	9/30/2005	Information Technology	Y
USM/CIO	TSA	$145,482	10/27/2004	Indefinite	TSA representative to the Information Technology Officer	N
USM/CIO	TSA	$138,093	4/3/2005	9/30/2005	Information Technology	Y
USM/CIO	TSA	$141,454	7/13/2003	Indefinite	INFRASTRUCTURE program support	Y
IAIP	USCG	$136,490	9/19/2003	9/19/2005	HSC Watch Augmentation	N

OGC	USCG	$82,937	3/1/2005	3/1/2007	Assist with international issues and with Team Telecom/CFIUS legal issues	N
USM/CFO	USCG	$101,613	8/1/2004	8/1/2005	Support Budget Office	N
USM/CFO	USCG	$82,937	1/5/2005	4/1/2005	ICE Tiger Team	N
USM/CIO	USCG	$156,886		Indefinite	Support DHS' Infrastructure Transformation Office	Y
IAIP	USCIS	$74,782	3/21/2005	5/21/2005	To assist in setting up DHS' Operations Center	N
IAIP	USCIS	$74,782	3/21/2005	5/21/2005	To assist in setting up DHS' Information Analysis Section	N
ICE	USCIS	$87,244	1/3/2005	Indefinite	To assist ICE in prosecuting Operation Jakarta Asylum Applications—detail lasts until this case goes to trial.	N
ICE	USCIS	$75,460	3/7/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
ICE	USCIS	$81,747	2/28/2005	3/4/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
ICE	USCIS	$41,361	3/7/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
ICE	USCIS	$64,981	3/14/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
BTS	USSS	$97,206	2/21/2004	8/21/2005	Border & Transp. Security	N
DHS/IAIP	USSS	$91,315	6/1/2004	12/1/2005	Investigations	N
FEMA	USSS	$91,315	10/17/2004	4/17/2005	DEST Program	N
FLETC	USSS	$68,651	8/1/2003	8/10/2008	Instructor	N
FLETC	USSS	$81,638	3/20/2005	3/20/2008	Instructor	N
FLETC	USSS	$68,651	1/1/2003	1/1/2006	Instructor	N
FLETC	USSS	$58,564	6/1/2000	6/1/2005	Instructor	N
FLETC	USSS	$81,638	2/1/2003	2/1/2006	Instructor	N
FLETC	USSS	$63,040	1/12/2004	1/12/2007	Instructor	N
FLETC	USSS	$81,638	2/9/2004	2/9/2009	Instructor	N
FLETC	USSS	$81,638	10/6/2002	12/6/2005	Instructor	N
FLETC	USSS	$81,638	9/1/2003	9/1/2006	Instructor	N
FLETC	USSS	$81,638	9/1/2003	9/1/2005	Instructor	N
IAIP	USSS	$84,751	10/19/2003	5/29/2005	Nat. CounterTerrorism Ctr	N
IAIP	USSS	UND—LT	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$77,274	3/13/2005	6/11/2005	HS Operations Center	N
IAIP	USSS	$100,152	1/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$114,344	5/7/2004	7/10/2005	Protective Research (IAIP)	N
IAIP	USSS	$40,179	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	UND—Off	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	11/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	5/1/2003	(3)	Support to IAIP mission	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
IAIP	USSS	$84,751	12/1/2002	([3])	Support to IAIP mission	N
IAIP	USSS	$97,206	2/8/2004	8/8/2005	Protective Research (IAIP)	N
IAIP	USSS	$103,947	9/1/2004	9/1/2005	Investigations	N
IAIP	USSS	$87,244	2/27/2005	5/28/2005	HS Operations Center	N
IAIP	USSS	$84,751	12/1/2002	([3])	Support to IAIP mission	N
IAIP	USSS	$110,878	6/1/2003	([3])	Support to IAIP mission—Investigations	Y
IAIP	USSS	$36,157	1/1/2004	([3])	Support to IAIP mission	N
IAIP	USSS	$117,809	12/1/2003	([3])	Support to IAIP mission	N
IAIP	USSS	$74,782	3/6/2005	6/4/2005	HS Operations Center	N
IAIP	USSS	$79,766	5/1/2004	5/1/2005	Investigations	N
IAIP	USSS	$100,152	10/1/2002	([3])	Support to IAIP mission	N
IAIP	USSS	$84,751	1/1/2004	([3])	Support to IAIP mission	N
IAIP	USSS	$117,809	1/1/2003	([3])	Support to IAIP mission	N
OSLGC	USSS	$88,000	10/3/2004	4/3/2005	Law Enforcement Liaison	N
S&T	USSS	$100,152	2/1/2003	Indefinite	Providing technical expertise to S&T	N
S&T	USSS	$97,206	1/1/2003	Indefinite	Providing technical expertise to S&T—Protective Research (INT)	N
Security	USSS	$97,206	7/21/2003	7/21/2005	Counter Intelligence	N
Security	USSS	$88,000	2/1/2003	Indefinite	Provides physical security to DHS facilities	N
Security	USSS	$94,000	2/23/2003	8/23/2005	Phy. Sec & Access Ctrl	N
USM/CHCO	USSS	$91,315	3/10/2004	4/1/2005	New HR system: pay and performance team	N
USM/CHCO	USSS	$82,259	2/1/2005	5/16/2005	Hiring and transition response team	N

[1] Indefinite.
[2] N/A.
[3] Ongoing.

HIRING JOURNALISTS

Question. In January 2005, President Bush ordered his Cabinet secretaries not to hire columnists to promote their agendas. At a news conference President Bush said, "All our Cabinet secretaries must realize that we will not be paying commentators to advance our agenda. Our agenda ought to be able to stand on its own two feet."

Are all DHS agencies in compliance with the Administration's policy and the legal prohibitions on using appropriations for contracting with journalists to promote legislation or policy?

Answer. Yes, all DHS Agencies are in compliance.

INTELLIGENCE REFORM BILL AUTHORIZATIONS

Question. The Intelligence Reform and Terrorism Prevention Act authorized substantial enhancements to a variety of DHS programs, including immigration enforcement, aviation security, and other provisions. Identify the funding requested in the President's fiscal year 2006 budget for each of the following authorizations contained in the Act. In your response, include a chart which compares the funding authorized, by section of the bill, to the funding included in the President's fiscal year 2006 budget.

Immigration Enforcement

—*Section 5202 & 5203.*—Authorizes, from fiscal year 2006 to fiscal year 2010 subject to the availability of appropriations, an increase of 10,000 additional Border Patrol Agents (2,000 per year) and an increase of 4,000 Immigration and Customs Enforcement (ICE) investigators (800 per year).

—*Section 5204.*—Authorizes, from fiscal year 2006 to fiscal year 2010 subject to the availability of appropriations, an increase of 40,000 beds (8,000 per year) available for immigration detention and removal.

—*Section 5101 through 5104.*—The Secretary of Homeland Security may carry out a pilot program to improve border security between ports of entry along the northern border. Required features of this pilot project include the use of advanced technologies to improve border security.

—*Section 5201.*—Within 6 months of enactment of this Act, the Secretary of Homeland Security shall submit a comprehensive plan for the systematic surveillance of the southwest border of the United States by remotely piloted aircraft.

—*Section 7210 & 7206.*—The bill amends the Immigration and Nationality Act by mandating by January 1, 2008 pre-inspection stations are established in at least 25 additional foreign airports and by December 31, 2006 at least 50 airports shall be selected for assignment of immigration officers to assist air carriers detect fraudulent documents at foreign airports. $25 million is authorized in fiscal year 2005 and $40 million in fiscal years 2006 and 2007 respectively for this purpose.

Aviation Security

—*Section 4013.*—$250 million for research, development, and installation of detection systems and other devices for the detection of biological, chemical, radiological, and explosive material.

—*Section 4024.*—$100 million for research and development of improved explosive detection systems.

—*Section 4052.*—$200 million for each of fiscal years 2005–2007 for improving aviation security related to the transportation of cargo on passenger and cargo aircraft.

—*Section 4052.*—$100 million for each of fiscal years 2005–2007 for research and development in advancing cargo security technology. Within these funds, the Secretary shall also establish a competitive grant program to encourage the development of advanced air cargo security technology.

—*Section 4014.*—Up to $150 million for each of fiscal years 2005 and 2006 to set up a pilot program (minimum 5 airports) to deploy and test advanced airport checkpoint screening devices and technology as an integrated system.

—*Section 4019.*—Increases the statutory allocation for expiring and new Letters of Intent (LOIs) from $250 million to $400 million.

—*Section 4011.*—$20 million for research and development of advanced biometric technology applications to aviation security, including mass identification technology.

—*Section 4011.*—$1 million for the establishment of a competitive center of excellence to expedite the use of biometric identifiers.

—*Section 4011.*—Directs that a law enforcement officer travel credential be created that incorporates biometric identifier technology that is uniform for all law enforcement officials seeking to carry a weapon on board an aircraft. The bill authorizes such sums as may be necessary to carry out this directive.

—*Section 4020.*—Directs DHS to provide, subject to the availability of funds, monitoring cameras for surveillance at airports that have checked baggage screening areas that are not open to public view in order to deter theft from checked baggage and to aid in the speedy resolution of liability claims against the Transportation Security Administration.

—*Section 4051.*—$2 million for TSA to carry out a pilot program to evaluate the use of blast-resistant containers for cargo and baggage on passenger aircraft to minimize the potential effects of detonation of an explosive device.

—*Section 4016.*—$83 million for the 3 fiscal-year period beginning with fiscal year 2005 to increase the number of Federal air marshals.

—*Section 4012.*—Directs TSA to begin to assume the function (not later than 180 days after testing the system is completed) of comparing passenger information to no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist, including international flights.

Other Provisions

—*Section 7303.*—Authorizes the Secretary of DHS to provide $22.1 million in fiscal year 2005, $22.8 million in fiscal year 2006, $23.5 million in fiscal year 2007, $24.2 million in fiscal year 2008, and $24.9 million in fiscal year 2009 to enhance public safety interoperable communications at all levels of government. The Secretary may establish an Office for Interoperability and Compatibility within the Science and Technology Directorate to carry out these duties.

—*Section 7304.*—Directs DHS to establish a minimum of 2 pilot projects in high threat urban areas or regions for the purpose of developing a regional strategic plan to foster interagency communication and to coordinate the gathering of all Federal, State, and local first responders in that area.

—*Section 7407.*—Amends the Homeland Security Act requirement related to counternarcotics enforcement. Instead of having one senior official in the Department coordinating counternarcotics policy, an "Office Counternarcotics Enforcement" is created with an authorization of $6 million.

—*Section 7215.*—Directs the Secretary to establish a terrorist travel program to oversee the analysis, coordination, and dissemination or terrorist travel intelligence and operation information.

—*Section 4071.*—Directs the Secretary to implement a system for screening the names of cruise ship passengers and crew against Federal terrorist watch lists.

Answer.

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 IMPLICATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY

Subject area	Authorized Funding Level	2006 Budget Funding Level
AVIATION:		
Law enforcement officer uniform biometric travel credential (Section 4011(a)).	Directs that a law enforcement officer travel credential be created that incorporates biometric identifier technology that is uniform for all law enforcement officials seeking to carry a weapon on board an aircraft. The bill authorizes such sums as may be necessary to carry out this directive.	The fiscal year 2006 Budget does not request any dedicated funding for this specific purpose. Necessary resources would be provided with existing funds or through fees. This activity is a sub-set of the Registered Traveler pilot and funds were identified within the Registered Traveler program in fiscal year 2005 to begin the Registered Armed LEO pilot. The fiscal year 2005 enacted appropriations funded Registered Armed LEO activities, and TSA anticipates using the results of the pilot as a platform for the final LEO biometric travel card. Results of the pilot will be considered to evaluate resources, needs, and funding options as the program moves forward.
Biometric technologies for aviation—R&D (Section 4011(b))	$20 million for research and development of advanced biometric technology applications to aviation security, including mass identification technology.	The fiscal year 2006 Budget does not request any dedicated funding for this specific purpose within broader R&D request levels.
Biometric Center of Excellence (Section 4011(d))	$1 million for the establishment of a competitive center of excellence to expedite the use of biometric identifiers.	The fiscal year 2006 Budget does not request any dedicated funding for a Biometric Center of Excellence.
Airline Passenger Screening (Section 4012)	Directs TSA to begin to assume the function (not later than 180 days after testing the system is completed) of comparing passenger information to no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist, including international flights.	The fiscal year 2006 Budget requests $81 million for the development of the Secure Flight prescreening system.
Checkpoint portal detection systems—R&D and deployment (Section 4013).	$250 million for research, development, and installation of detection systems and other devices for the detection of biological, chemical, radiological, and explosive material.	The fiscal year 2006 Budget for explosives detection as a countermeasure against aviation, suicide and vehicle bombs: $88 million of the $124 million (Research and Development (R&D) consolidation budget + Science and Technology (S&T) Explosives Countermeasures portfolio budget), but nothing specific for ''checkpoint portal detection systems''.

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 IMPLICATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY—Continued

Subject area	Authorized Funding Level	2006 Budget Funding Level
Integrated checkpoint screening system pilots (Section 4014)	Up to $150 million for each of fiscal years 2005 and 2006 to set up a pilot program (minimum 5 airports) to deploy and test advanced airport checkpoint screening devices and technology as an integrated system.	The President's fiscal year 2005 Budget included $28.3 million for fielding emerging technology equipment at checkpoints. As a result of this funding, 147 static trace portals (which are passenger screening sub-systems using a whole body portal to inspect passengers for concealed explosives using an automated, non-contact trace sampling and processing system) will be deployed in fiscal year 2006 at approximately 40 airports. The fiscal year 2006 request includes $43.7 million in additional funds to complete the fielding of this capability, which will total $100 million to address this activity over the 2-year period.
In-line checked baggage screening (Section 4019)	Increases the statutory allocation for expiring and new Letters of Intent (LOIs) from $250 million to $400 million.	The fiscal year 2006 Budget includes $260.5 million to support the eight existing Letters of Intent (LOI) airports. Of this amount, $240.5 million is for direct reimbursements and $20 million is for equipment and installation. The fiscal year 2006 request proposes to continue sourcing LOIs from the $250 million appropriated from the Aviation Security Capital Fund at a 75 percent Federal cost share rate. Additionally, the request includes $134 million to purchase and install Explosive Detection Systems and Electronic Trace Detection equipment at non-LOI airports, for a total expenditure of $394 million.
Checked Baggage Monitoring Area (Section 4020)	Directs DHS to provide, subject to the availability of funds, monitoring cameras for surveillance at airports that have checked baggage screening areas that are not open to public view in order to deter theft from checked baggage and to aid in the speedy resolution of liability claims against the Transportation Security Administration. The bill and current policy provides "such sums".	The fiscal year 2006 Budget includes $10.1 million to provide assistance to airports to install security monitoring cameras for surveillance of checked baggage screening areas that are not open to public view. The Transportation Security Administration (TSA), in partnership with airports, generally provides for purchase and installation of a camera system, with the partnering airport agreeing to maintain the installed system.
Aviation explosives detection equipment R&D (Section 4024(b))	$100 million for research and development of improved explosive detection systems.	The S&T Directorate has an fiscal year 2006 budget request of $45.9 million for the TSA budget line for next generation explosives detection systems. The S&T Directorate will coordinate with TSA regarding the development of the next generation of explosives detection systems.

Blast Resistant Cargo Containers (Section 4051)	$2 million for TSA to carry out a pilot program to evaluate the use of blast-resistant containers for cargo and baggage on passenger aircraft to minimize the potential effects of detonation of an explosive device.	The fiscal year 2006 Budget requests $4.4 million.
Air cargo security activities (Section 4052)	$200 million for each of fiscal years 2005–2007 for improving aviation security related to the transportation of cargo on passenger and cargo aircraft. $100 million for each of fiscal years 2005–2007 for research and development in advancing cargo security technology. Within these funds, the Secretary shall also establish a competitive grant program to encourage the development of advanced air cargo security technology.	The fiscal year 2006 Budget includes $40 million for air cargo security, which will allow the Transportation Security Administration (TSA) to continue making incremental and measured progress toward our air cargo security goals. The S&T Directorate has an fiscal year 2006 budget request of $29.578 million. The budget request, although not developed by the S&T Directorate, was agreed upon by the S&T Directorate as the amount moving forward for air cargo RDT&E. The S&T Directorate will continue to award grants under a competitive process to further aviation consolidated cargo screening RDT&E.
Federal Air Marshals (FAMS) staffing (Section 4016)	$83 million for the 3 fiscal-year period beginning with fiscal year 2005 to increase the number of Federal air marshals. Subject to the availability of appropriations.	The President has requested $9.86 million in new funding in fiscal year 2006 to enable the hiring of additional Federal Air Marshals to provide even greater coverage of targeted critical flights and to otherwise increase mission capabilities. The total budget for FAMS is $689 million.
Pre-clearance Stations and Immigration Security Initiative (Section 7210 & 7206).	The bill amends the Immigration and Nationality Act by mandating by January 1, 2008 pre-inspection stations are established in at least 25 additional foreign airports and by December 31, 2006 at least 50 airports shall be selected for assignment of immigration officers to assist air carriers detect fraudulent documents at foreign airports. $25 million is authorized in fiscal year 2005 and $40 million in fiscal years 2006 and 2007 respectively for this purpose.	There are currently 14 pre-clearance stations funded in the fiscal year 2006 Budget. The fiscal year 2006 Budget request is $2 million

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 IMPLICATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY—Continued

Subject area	Authorized Funding Level	2006 Budget Funding Level
MARITIME:		
Vetting of cruise ship passengers (Section 4071)	Directs the Secretary to implement a system for screening the names of cruise ship passengers and crew against Federal terrorist watch lists. No specific funding authorization is provided.	The fiscal year 2006 Budget does not request any dedicated funding for this specific purpose. Necessary resources are provided with existing funds. On April 7, 2005, CBP published the Advance Passenger Information System (APIS) Final Rule within the Federal Register (70 FR 17820). The CBP Final Rule incorporates passenger and crew manifest requirements from CBP with the Notice of Arrival requirements of the United States Coast Guard (USCG). The CBP Final Rule requires that sea carriers electronically submit certain data on all passengers and crew members prior to entry to or departure from the United States. The data that must be provided includes biographical data and vessel information for each passenger or crewmember. Working with the USCG, CBP developed the Electronic Notice of Arrival/Departure System (eNOA/D), an Internet portal available on the National Vessel Movement Center (NVMC) web site. Using this portal, commercial vessel owners, operators or agents can transmit one electronic message and comply with the CBP APIS requirement for passengers and crew and the USCG Notice of Arrival requirements for vessels. eNOA/D became operational and available to the industry during February 2005. CBP's efforts on the eNOA/D system have been accomplished with existing funds.

BORDER PROTECTION:		
Advanced Technology Northern Border Security Program (Section 5101–5104).	The Secretary of Homeland Security may carry out a pilot program to improve border security between ports of entry along the northern border. Required features of this pilot project include the use of advanced technologies to improve border security. There is authorized to be appropriated ''such sums as may be necessary to carry out the pilot program''.	The fiscal year 2006 Budget does not request any dedicated funding for a specific pilot. Necessary resources will be provided with existing funds. The fiscal year 2006 Budget requested funding for $19.8 million added to the base funding of $31.3 million to improve border security using advanced technologies on both the northern and southern land borders. Also included in the fiscal year 2006 CBP budget are $20 million for aircraft recapitalization, $10 million in base funding for UAVs, and funding for technical infrastructure. The America's Shield Initiative (ASI) program will evaluate and determine the optimal mix of technology for meeting security requirements of both land borders.
Border surveillance (Section 5201)	Within 6 months of enactment of this Act, the Secretary of Homeland Security shall submit a comprehensive plan for the systematic surveillance of the southwest border of the United States by remotely piloted aircraft. The Secretary of Homeland Security shall implement the plan as a pilot program as soon as sufficient funds are appropriated and available for this purpose.	The fiscal year 2006 Budget requests $10 million for unmanned aerial vehicles.
Border Patrol agents (Section 5202)	Authorizes, from fiscal year 2006 to fiscal year 2010 subject to the availability of appropriations, an increase of 10,000 additional Border Patrol Agents (2,000 per year).	The fiscal year 2006 Budget requests 210 new agents and $36.9 million.
ENFORCEMENT:		
Immigration and Customs Enforcement investigators (Section 5203)	Authorizes, from fiscal year 2006 to fiscal year 2010 subject to the availability of appropriations, an increase of 4,000 Immigration and Customs Enforcement (ICE) investigators (800 per year). Subject to the availability of appropriations.	The fiscal year 2006 Budget requests 150 agents and $18 million.
Detention bed space (Section 5204)	Authorizes, from fiscal year 2006 to fiscal year 2010 subject to the availability of appropriations, an increase of 40,000 beds (8,000 per year) available for immigration detention and removal. Subject to the availability of appropriations.	The fiscal year 2006 Budget includes an increase of $90 million for detention beds and detention and removal officers. This increase will fund 1,920 beds. Overall, the fiscal year 2006 Budget provides $1.5 billion for detention and removal activities. The budget also includes an enhancement of $39 million for the detention and repatriation costs of the Arizona Border Control Initiative.

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 IMPLICATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY—Continued

Subject area	Authorized Funding Level	2006 Budget Funding Level
OTHER:		
Public Safety Interoperable Communications (Section 7303)	Authorizes the Secretary of DHS to provide $22.1 million in fiscal year 2005, $22.8 million in fiscal year 2006, $23.5 million in fiscal year 2007, $24.2 million in fiscal year 2008, and $24.9 million in fiscal year 2009 to enhance public safety interoperable communications at all levels of government. The Secretary may establish an Office for Interoperability and Compatibility within the Science and Technology Directorate to carry out these duties.	The fiscal year 2006 Budget requests $20.5 million for the S&T Directorate's Office of Interoperability and Compatibility (OIC) to enhance public safety interoperable communications.
Regional Strategic Plan (Section 7304)	Directs DHS to establish a minimum of 2 pilot projects in high threat urban areas or regions for the purpose of developing a regional strategic plan to foster interagency communication and to coordinate the gathering of all Federal, State, and local first responders in that area.	The fiscal year 2006 Budget requests $20.5 million for the Department of Homeland Security's S&T Directorate's OIC to enhance public safety interoperable communications through SAFECOM, a program of OIC.
Counternarcotics Enforcement (Section 7407)	Amends the Homeland Security Act requirement related to counternarcotics enforcement. Instead of having one senior official in the Department coordinating counternarcotics policy, an ''Office Counternarcotics Enforcement'' is created with an authorization of $6 million.	The fiscal year 2006 request for the Office of Counternarcotics Enforcement is $1.86 million.
Terrorist Travel Program (Section 7215)	Directs the Secretary to establish a terrorist travel program to oversee the analysis, coordination, and dissemination or terrorist travel intelligence and operation information.	The fiscal year 2006 Budget does not request any dedicated funding for this specific purpose. Necessary resources would be provided with existing funds.

MERIT SYSTEM PROTECTION BOARD (MSPB)

Question. The final regulation restricts the ability of the MSPB to mitigate penalties selected by DHS. The final rule says, "Our intent is to explicitly restrict the authority of MSPB to modify those penalties to situations where there is simply no justification for the penalty. MSPB may not modify the penalty imposed by the Department unless such penalty is so disproportionate to the basis for action as to be wholly without justification." This standard is exceptionally high. Why was such a departure from the current authorities of the MSPB necessary?

Answer. Under current MSPB case law, penalties can be mitigated down if they are "unreasonable." Problems with this include that it is subjective and it may result in many employees returning to the workplace after the MSPB "suspension" instead of being removed as recommended by management.

DHS believes that management decisions should be given great deference with regard to discipline, especially with removals, because an undesirable employee returning to the workforce creates morale problems at the least; at the worst, a returning employee interferes with the agency's mission to protect the homeland.

MSPB's ability to mitigate a penalty only if the punishment is "so disproportionate as to be wholly without justification" is a compromise because it gives greater deference to DHS, still protects employee due process, and ensures that disciplinary actions are not initiated irresponsibly.

Question. Is the Department concerned that these extreme measures will adversely affect employee morale and reduce employee confidence that they will be treated fairly?

Answer. DHS understands that many employees are wary of the unknown and is currently in the process of rolling out significant training efforts aimed at communicating with employees, training managers, and executives on the new human resource system and the expectations for those managers regarding the system. Fair treatment is critical to the success of the new system and is a key component of our implementation and ongoing evaluation processes.

Question. What evidence is there that the existing MSPB authorities have adversely affected agency missions?

Answer. The Department's priority homeland security mission requires that it maintain an exceptionally high degree of order and discipline in the workplace. This order and discipline is undermined when disciplinary decisions are mitigated by MSPB judges on the existing "reasonableness" standard. Indeed, the mere threat of such a low standard for mitigation causes agency managers to second guess themselves and hesitate to discipline employees even when such discipline is clearly warranted. The Department has therefore instituted a higher standard for mitigation of penalties aimed at providing managers with the confidence to institute disciplinary actions where required in support of the agency's homeland security mission. To allow very poor performers to continue in the workplace is unacceptable and can negatively affect all agency operations.

CONCERNS OF EMPLOYEES

Question. A number of DHS employees have strong concerns about the final DHS personnel regulations, which were published in the Federal Register on February 1, because the regulations diminish employees due process rights and restrict collective bargaining. What is the Department's opinion on the objections raised by the front line DHS employees, and what will the Department do to address the concerns expressed by these Federal employees?

Answer. The new HR system does maintain due process and is consistent with the Homeland Security Act's promise to preserve collective bargaining rights. It also is responsive to DHS' unique mission needs. DHS understands that employees have concerns about the new human resources systems and has embarked on robust efforts to inform employees and train managers about the new system, including through continuing collaboration with DHS labor unions. Through focus groups, the "Ask MAX" question response system and employee surveys, DHS is keeping a close watch on employee opinions and through the formal program evaluation process will be measuring the results and outcomes of the new system. If necessary, the system can be fine-tuned to make mid-course corrections.

INDEPENDENT REVIEW OF COLLECTIVE BARGAINING DISPUTES

Question. As part of the new personnel regulations, the responsibility for deciding collective bargaining disputes will lie with a three-member internal DHS Labor Relations Board appointed by the Secretary. Currently, throughout the Federal Government, collective bargaining disputes are decided by the Federal Labor Relations

Authority (FLRA), an independent body appointed by the President and confirmed by the Senate. How does DHS/OPM believe that the internal labor relations board meets the statutory mandate of the Homeland Security Act that DHS employees may, "organize, bargain collectively, and participate through labor organizations of their own choosing in decisions which affect them"?

Answer. The Homeland Security Labor Relations Board (HSLRB) is an independent Board similar to the FLRA, but appointed by the Secretary with nominees recommended by the DHS labor organizations. All nominees must be independent citizens who are known for their integrity and impartiality in addition to having expertise in labor relations, law enforcement, or national/homeland or other related security matters. The HSLRB hears cases involving the duty to bargain and the DHS homeland security mission, with the FLRA hearing all other cases (for example, appropriate unit determinations and unfair labor practice charges involving exercise of employee rights) and reviewing the HSLRB's substantive decisions. The FLRA review is then subject to judicial review. These substantive and procedural attributes of the HSLRB ensure that DHS, DHS employees and DHS labor organizations obtain an impartial adjudication of labor relations cases while recognizing the Department's priority homeland security mission.

MANDATORY TERMINATION WITH NO OUTSIDE REVIEW

Question. The final regulations provide the Secretary with discretion to create a list of Mandatory Removal Offenses (MRO) that will only be appealable on the merits to an internal DHS Mandatory Removal Panel (MRP) appointed by the Secretary. In addition, the regulations provide the Secretary with the sole discretion to mitigate a removal penalty. How can the agency expect front line employees to have any confidence in a personnel system where the most serious matters are charged and adjudicated by the Secretary and his appointed "Removal Panel"?

Answer. Currently DHS is taking no action to implement MROs. On August 15, 2005, Judge Collyer of the District Court for the District of Columbia requested that DHS and OPM delay implementation. On August 12, 2005, Judge Collyer issued an order enjoining one provision within the appeals subpart of the regulations but permitting DHS to move forward with the rest of the adverse actions and appeals provisions. The Department and OPM are currently working to set a revised timeline for making the adverse actions and appeals subparts operative in light of the ruling.

TASKING THE FLRA AND MSPB

Question. What particular statutory authority enabled the final regulations to give the FLRA and the MSPB new duties and rules of operation? The FLRA and the MSPB are independent agencies.

Answer. The Homeland Security Act provided an amendment to Title 5, United States Code, that authorized the Secretary of DHS and the Director of OPM to establish a human resources management system for DHS that waives or modifies certain provisions of Title 5. Included among the provisions that can be waived or modified are chapters 71 and 77, which prescribe the operations of the FLRA and MSPB respectively. After consulting with FLRA and MSPB, the Secretary and the Director relied upon this grant of authority, found in 5 U.S.C. 9701, to promulgate regulations that modify chapters 71 and 77 and alter the way the FLRA and MSPB handle DHS cases.

TRAINING OF SUPERVISORS

Question. One of the continuing concerns surrounding the final DHS personnel regulations is the fact that many personnel decisions, especially pay, will now be based on factors under the control of local supervisors and directors. How does DHS plan to address the concerns of front line officers that supervisors, who will be granted a tremendous amount of pay and performance evaluation discretion under the new personnel regulations, will be properly trained to ensure transparency and fairness for all front-line personnel?

Answer. Performance ratings will continue to be determined by local supervisors, just as it occurs in today's performance management process. The concept of a second level reviewing official has been retained as an inherent check and balance. A comprehensive training program will be undertaken to train supervisors and managers to make meaningful distinctions in performance and, just as important, to articulate clear performance expectations, which will be used to track performance. An automated performance management system will make the administration of the system more transparent to employees and will facilitate self-assessment and peer review capabilities that can serve as important information sources for the supervisor's consideration. Additionally, we envision that performance pay pools will be

centrally established and managed at higher organizational levels, thus mitigating the influence of a single supervisor on the pay side of the process. A Department-level Compensation Committee, including DHS union representation, also will have considerable influence on the pay for performance program and its administration.

Question. In addition, this system will take more training and administrative time. How will those increased administrative costs be paid for?

Answer. The vast majority of administrative costs associated with training will be funded through requested appropriations specified for implementation of the new HR system and managed by the DHS Chief Human Capital Office for the Department-wide training initiative. As part of the new system, DHS will provide automated tools, e.g., a new electronic performance management system, to assist management officials in program administration.

Question. Won't resources be taken from frontline Homeland Security positions?

Answer. The expectation is that resources will be provided in requests for appropriations specifically identified to support implementation of the new HR system. Individual Department components' mission budgets are not expected to be impacted. We believe time spent in training on effective performance management and in coaching and providing feedback to employees is time well spent that generates positive returns in overall agency effectiveness.

PAY FOR PERFORMANCE

Question. As you know, DHS employees' pay will be shifting from the current GS-scale pay system to a pay-for-performance system under the new DHS personnel regulations. How can a credible pay-for-performance pay system work in an agency, such as DHS, that requires a tremendous amount of teamwork to successfully accomplish agency missions?

Answer. Performance work plans will contain measurable performance elements that specifically address teamwork or similar concepts for those occupations requiring such attributes. Employees in those occupations will know that performance that demonstrates teamwork will be rewarded.

Question. Is the Department aware of any large scale pay-for-performance system that has been successfully implemented in a law-enforcement environment?

Answer. While we are unaware of a large scale pay-for-performance system in a law enforcement environment, that certainly does not prevent us from developing one. Pay-for-Performance is the concept of providing a pay increase based on "performance" (e.g. achievement of a performance goal or positive performance appraisal rating). Organizations tie pay to performance in various ways. They may base pay on measures of individual, team, or organizational performance. We feel this concept can work well in a law enforcement environment. Research involved in designing the system entails review and evaluation of private, other Federal, State and local systems that have such programs. Our design work includes program evaluation aspects in order to periodically monitor, evaluate, and revise the system, as warranted to ensure that objectives are being attained.

SECURITY AND PROSPERITY PARTNERSHIP OF NORTH AMERICA

Question. On March 23, President Bush held a press event in Waco, Texas with Mexican Pres Foxx and Canadian Prime Minister Martin where he announced a grant program for the Security and Prosperity Partnership of North America.

The parties to the partnership were tasked to set specific, measurable, and achievable goals and implementation dates to develop a common security strategy to further secure North America, including preventing and responding to threats within North America and streamlining the secure and efficient movement of legitimate and low-risk traffic across our shared borders.

Will we be receiving a budget amendment to provide the resources for Customs and Border Patrol, the Coast Guard, and Immigration and Customs Enforcement to implement this partnership or was this announcement an exercise in public relations?

Answer. On March 23, 2005, in Waco, Texas, President Bush, along with Canadian Prime Minister Martin and Mexican President Fox, unveiled the Security and Prosperity Partnership for North America (SPP), a blueprint for a safer and more prosperous continent. The three leaders instructed each nation to establish ministerial-level SPP working groups. I chair the security component, and the prosperity component is chaired by Department of Commerce Secretary Gutierrez. Department of State Secretary Rice is working to ensure the two components are integrated and that the SPP advances U.S. foreign policy goals and enhances our strong relationships with Canada and Mexico.

The SPP will complement, rather than replace, existing bilateral and trilateral fora and working groups that are performing well. The issues of immigration and trade disputes will be dealt with outside the SPP through existing treaties and congressional action.

Following the March 23 announcement, DHS and Commerce conducted a series of Congressional briefings and other stakeholder outreach sessions.

On June 27, I and Gutierrez and our government counterparts in Mexico and Canada released the first report of the SPP that identifies initial results, key themes and initiatives, and work plans that further promote the security and prosperity of the continent.

At this time, DHS anticipates accomplishing the fiscal year 2006 initiatives contained in the SPP within available resources. We would like to reserve the opportunity to address some longer term priorities as part of the normal budgeting process in the future. We continue to be interested in input from the Congress, industry and other stakeholders as we implement the SPP.

DHS REPORTS DUE

Question. In the fiscal year 2005 Homeland Security Appropriations Act and associated reports, Congress directed the Department to report to the Committee on a number of important issues. To date, 70 percent of the reports currently due to the House & Senate Committees on Appropriations have not yet been received. What is the Department's plan for increasing the rate of timely submission of Congressionally required reports?

Answer. The Department continues to place a significant priority on providing timely information and reports to Congress. Of the reports mentioned above, approximately 40 percent of those outstanding reports are past due, and the Department has been working diligently to expedite transmittal of those reports. Since the hearing on April 20th through July 13th, the Department has reduced the overall number of outstanding reports by approximately 30 percent. As of July 13, the Department has submitted 143 reports for fiscal year 2005 to the Congressional Appropriation Committees.

The status of reports is constantly monitored and regular progress is tracked and evaluated. Furthermore, Congressional reports are discussed regularly at several high-level management meetings, including the DHS Management Council, Chief Financial Officers Council, and Budget Officer meetings. In addition, the Department has reviewed and implemented strategies to streamline and improve the clearance process.

CHIEF INFORMATION OFFICER

Question. From the fiscal year 2004 enacted budget to the fiscal year 2006 President's request, the CIO's budget has increased substantially. The President's budget for fiscal year 2006 requests $303.7M for this office. What safeguards has the Department put in place to ensure that this funding has the proper government management and oversight?

Answer. The Department is using two parallel processes to ensure proper governance and management of its funding, the Planning, Programming, Budgeting, and Execution (PPBE) process, mandated by Management Directive (MD) 1330, and the Investment Review Process (IRP), mandated by MD 1400.

The PPBE process has four steps:

—*Planning.*—The Office of the CIO (OCIO) develops information technology (IT) strategic plans and these plans are reviewed to ensure alignment with the Department's overall strategic plan.

—*Programming.*—The OCIO enters its budget year plus 4 years funding requirements into the Future Years Homeland Security Program (FYHSP) system for review, program evaluation, and analysis by Departmental management.

—*Budgeting.*—The OCIO budget is reviewed and the OCIO enters budget justification information for all of its IT investments into the Investment Management System (IMS) for scoring and portfolio review by Departmental management.

—*Execution.*—All spending plans are reviewed before and during the execution year by Departmental management. Also, each individual expenditure is reviewed at multiple Levels within the OCIO and by Departmental management before execution, and is tracked through the Federal Financial Management System (FFMS) and the Procurement Request Information Management System (PRISM).

The Investment Review Process (IRP) consists of a layered review process, depending on the Level and life cycle phase of the investment. Specifically, the IRP consists of the following:

—*Investment Review Board (IRB).*—The IRB provides decision authority for Level 1 investments that have an acquisition cost of over $100 million and IT investments with a life cycle cost of over $200 million.

—*Joint Requirements Council (JRC).*—The JRC provides decision authority for Level 2 investments that have an acquisition cost between $50 million and $100 million, and IT investments with a life cycle cost between $100 million and $200 million.

—*Enterprise Architecture Board (EAB).*—The EAB conducts a full review of Level 3 IT investments with an acquisition cost between $5 million and $50 million, and a life cycle cost between $20 million and $100 million and conducts a limited review of Level 4 IT investments (investments with an acquisition cost below $5 million and a life cycle cost below $20 million). The EAB operates within the OCIO and ensures the existence of an effective IT governance process in accordance with DHS architecture principles. As part of its overall governance strategy, the EAB conducts milestone reviews of investment initiatives to help manage architectural alignment within DHS and serve as the conduit for receiving, analyzing, and disseminating information. This process also supports the DHS CPIC (Capital Planning and Investment Control), acquisition, and budget processes, and serves to identify, evaluate, select, align, and approve investments, technologies, and policies for use in DHS.

MEETING WITH UNIONS

Question. During your confirmation hearing on February 2, 2005, you testified that you would meet with the representatives of the various union members working in the Department. Have you met with the unions?

Answer. Yes. In April, I met with the President of the National Treasury Employees Union (NTEU) and the President of the American Federation of Government Employees (AFGE). These are the two largest unions represented in DHS, and the only two with national consultation rights at the Department.

HEARINGS ON THE PATRIOT ACT

Question. The PATRIOT Act was enacted in haste, with minimal debate, in a time of crisis.

Legislation called the SAFE Act has been introduced by Senators Feingold, Craig, Durbin and others to modify certain provisions of the PATRIOT Act. While I support review of the provisions referenced in the SAFE Act, I would prefer that all provisions of the law be subject to examination in hearings held by all relevant committees of jurisdiction in the House and Senate. This law was never subject to substantial debate. In prior meetings with you, you have assured me that you would support hearings on the Patriot Act.

Do you continue to support broad ranging hearings to examine, in depth, the provisions of the PATRIOT Act?

Answer. The USA PATRIOT Act provides invaluable tools for protecting Americans from terrorist attacks while safeguarding civil liberties and preserving the important role of congressional and judicial oversight. The USA PATRIOT Act has been the subject of numerous hearings in the Congress. I am committed to working with Congress on all issues that relate to the Department, including matters, like the USA PATRIOT Act, that are crucial to terrorism prevention.

INFORMATION CONCERNING THE PATRIOT ACT

Question. As you know, when the PATRIOT Act was enacted, the Congress included sunsets on certain surveillance powers so the Congress could evaluate how those powers had been used before deciding wether to extend them or make them permanent. Some of those provisions scheduled to expire at the end of this year are not controversial. Other provisions are controversial, and some that are not even subject to sunset have been criticized for infringing on the privacy rights and civil liberties of law-abiding American citizens.

Are you committed to working with the Congress to ensure that we have the information we need from the Administration and the Department of Homeland Security in particular, so the Congress may make an informed decision about whether to renew those provisions that will expire at the end of this year or make other changes to the PATRIOT Act?

Answer. I am committed to ensuring that the Department continues to provide Congress with the appropriate information it needs.

CONSULTING WITH CONGRESS

Question. Attorney General Ashcroft engaged in minimal consultation with the Congress and members on both sides of the aisle on the PATRIOT Act and other key pieces of legislation considered in the wake of 9/11. A full draft bill, known as PATRIOT II, became public before any discussions with interested Members of Congress had taken place, and while the proposed bill was later disavowed as merely a draft, many of the proposals contained in it were subsequently included in other Administration proposals.

Now that you have been confirmed, will you continue to consult closely with Congress and Members on both sides of the aisle before rolling out new legislative proposals to expand Federal law enforcement, surveillance, and other powers that might curtail constitutional rights and protections?

Answer. I will continue to engage actively in the consultation process as we seek to offer new programs and legislative proposals.

Question. What actions are you taking in your role as head of the Department of Homeland Security to ensure that such consultation occurs?

Answer. I have conveyed to the DHS Senior Leadership and the appropriate offices within the Department of the importance of consulting with Congress and keeping Members informed of programs, policy, and operational activities within the Department. My expectation is that they will do so in a timely fashion.

SECURE FLIGHT

Question. On March 28, 2005, the Government Accountability Office (GAO) released a report entitled, "Secure Flight Development and Testing Under Way, but Risks Should be Managed as System Is Further Developed". The GAO was mandated to do this report by the fiscal year 2005 Homeland Security Appropriations Act. In essence, the report found that Secure Flight is not ready for primetime. Only one of the ten specific aspects of the development and implementation of Secure Flight has been met.

Mr. Secretary, I want to make the skies safer for all passengers who fly on commercial aircraft. But I also want to ensure that those individuals who fly have their legitimate privacy rights and civil liberties protected. And I want to ensure that whatever pre-screening system is developed is safe from abuse by outside or unauthorized entities. My main concern with Secure Flight—and its predecessors—is that I have not yet been convinced that these protections are in place. Indeed, the GAO has not yet been convinced either. Four of the ten areas the Congress mandated the GAO review are specifically focused on privacy, safety and redress. The best that the GAO can say about the status of these items is that they are "under way".

It is not yet clear that the new Secure Flight program will create a redress process for passengers to correct erroneous information, nor is it clear that it will include security measures to protect the system from unauthorized access.

Over $130 million and more than 3 years have been spent to date on Secure Flight and its predecessors. I understand your plan is to begin initial testing of this program late this summer using passenger data from two airlines. If in April 2005 the best that can be said of the program is that it is "under way", what will be the likelihood that Secure Flight will truly be "under way" in August 2005?

Answer. As we have stated, TSA intends to have Secure Flight underway later in 2005. At the request of the air carriers, TSA shifted its planned August launch date to September to account for the busy Labor Day holiday travel weekend. In addition, TSA made further adjustments to the implementation plan for Secure Flight to ensure that all regulatory and privacy documents comply with all applicable statutes and guidelines, as well as airline requests regarding technical guidance. In addition, the decision not to include commercial data in the initial rollout of Secure Flight caused further adjustments in the schedule, as did the ongoing uncertainty regarding the program's budget for fiscal year 2006. Under the revised implementation schedule, TSA expects to be in compliance with the requirement of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) to implement passenger prescreening within 180 days of completion of testing.

Question. Mr. Secretary, can you commit to us that Secure Flight will not be deployed until all ten of these areas of concern are addressed?

Answer. TSA is working to meet the deadline in the IRTPA to begin to assume the watch list screening function from air carriers. As we move forward, TSA is continuing to cooperate with GAO to address the outstanding policy and operational items the agency is required to resolve under the Homeland Security Appropriations Act, 2005 (Public Law 108–334), prior to implementation. TSA will show that it has

addressed those items, as well as each of the additional GAO recommendations in its March 2005 report, prior to deployment of the program.

Question. In recent weeks, data storage systems for major companies which track and store commercial data on individual citizens have been compromised. Both ChoicePoint and LexisNexis have admitted that their databases have been accessed by unauthorized, outside entities—potentially exposing hundreds of thousands of Americans to identity theft. I have long been concerned about the privacy implications for citizens by the possible use of commercial databases for passenger screening activities. These unauthorized intrusions by outside hackers and other unscrupulous individuals only serve to enhance my concerns. The GAO has noted that Secure Flight's system safeguards and other protections from unauthorized access have not yet been developed nor tested. However, I understand that the use of commercial databases, such as these, remain under consideration for the purpose of verifying a potential traveler's identity.

Given these recent incidents, are you reconsidering the use of commercial databases?

Answer. TSA conducted a very limited test to determine whether the use of commercial data could improve the effectiveness of the watch list comparisons undertaken in the Secure Flight program as well as to assist with the identification of passenger information that is incorrect or inaccurate.

In the Homeland Security Appropriations Act, 2005 (Public Law 108–334, Section 522(d)), Congress mandated that prior to commercial data testing, TSA would be required to develop measures to assess the impact of using commercial data on aviation security, and that the GAO is to review those measures. TSA is complying with all Congressional requests on this issue and the GAO will continue to evaluate TSA's development of performance measures throughout the test phases.

TSA's testing of the use of commercial data is governed by privacy and data security protections, including strict prohibitions on the use of any passenger information provided by commercial data sources. TSA will not incorporate the use of commercial data into Secure Flight unless testing confirms that:

—it enhances security;
—it does not result in inappropriate differences in treatment of any category of persons; and
—robust data security safeguards and privacy protections can be put in place to ensure that commercial entities do not gain wrongful access to or use passenger personal information inappropriately.

TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Results of the testing, the comparisons of Passenger Name Record (PNR) information against names in the Terrorist Screening Database and the use of commercial data, will be as publicly transparent as possible without compromising national security. Testing and eventual implementation will be governed by strict privacy protections including passenger redress procedures, data security mechanisms, and limitations on use.

Question. What can be done to ensure the security of these databases and the integrity of the system?

Answer. TSA conducted a very limited test to determine whether the use of commercial data could improve the effectiveness of the watch list comparisons undertaken in the Secure Flight program as well as to assist with the identification of passenger information that is incorrect or inaccurate.

TSA's testing of the use of commercial data is governed by privacy and data security protections, including strict prohibitions on the use of any passenger information provided by commercial data sources. TSA will not incorporate the use of commercial data into Secure Flight unless testing confirms that:

—it enhances security;
—it does not result in inappropriate differences in treatment of any category of persons; and
—robust data security safeguards and privacy protections can be put in place to ensure that commercial entities do not gain wrongful access to or use passenger personal information inappropriately.

TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Results of the testing, the comparisons of PNR information against names in the Terrorist Screening Database and the use of commercial data, will be as publicly

transparent as possible without compromising national security. Testing has been governed by strict privacy protections including data security mechanisms, and limitations on use. Secure Flight has a written data control policy for this very purpose. All personnel who handle passenger data are required to sign a Non Disclosure Agreement (NDA) specific to the Secure Flight program and must successfully complete a privacy training course. Accountability for data is accomplished by assigning a control number to each disk, tape, or document on which the data is stored. In addition, a Chain of Custody process is in place to record and track data transfers by hand receipt. Finally, stand alone Government Furnished Equipment (GFE) has been identified to be used on this project. Authorization to load/install/read any PNR data is restricted to GFE designated and documented to process PNR data, and none of those machines is capable of transmitting data outside of the facility.

The Commercial Data Test also required the contractor to comply with the security requirements, regulations, and privacy protections for all records used, accessed, or contacted, as well as the data handling procedures in the Security Standard Operating Procedures and the Data Security and Control Policy. The contractor is required to comply with security requirements to maintain their Secure Facility Clearance.

Finally, the Secure Flight system will be subject to certification and accreditation prior to achieving Authority to Operate (ATO) in early fall 2005. TSA and DHS Chief Information Security Officers require all information and system security is in working order prior to ATO of the initial operating capability with initial air carriers.

SECURE FLIGHT—MOVEMENT TO SCO

Question. What impact will moving the operation of Secure Flight to the proposed Screening and Credentialing Operations office have on its implementation?

Answer. We support the concept of a Screening Coordination and Operations (SCO) Office, and requested, through the 2SR process, recommendations to best meet the goals of the office. Consistent with the 9–11 commission recommendations, HSPD–11 and HSPD–12, the SCO office would support the development of a more unified, comprehensive and efficient system for the screening, credentialing, and redress for passengers, while leveraging and optimizing investments in screening systems and tools. The SCO would be supported by a management approach that would lead to harmonized IT architecture, uniform redress, and provision of coordinated or shared services such as card production, biometric/biographic databases, and global enrollment systems/processes that adhere to standards set by DHS with close linkage to policy decisions and overall information technology enterprise architectures. The SCO office would also ensure a consistent approach also for outreach in the areas of privacy, civil rights, and helping to ensure coordinated R&D efforts. DHS plans to set up the SCO office in fiscal year 2006.

Question. Do you have concerns that further rearranging the organizational chart will further slow the development and operation of Secure Flight?

Answer. The exact roles, responsibilities, and composition of the SCO are currently under review and further definition and refinement of the SCO concept will be developed based on that review. An implementation and transition plan for the SCO will also be developed based on that review.

Question. If it is moved, who will actually maintain and operate the system—the SCO or TSA?

Answer. The exact roles, responsibilities, and composition of the SCO are currently under review and further definition and refinement of the SCO concept will be developed based on that review.

Question. Have you experienced any delays in receiving timely security information from the Terrorist Screening Center (which is run by the FBI) for Secure Flight or your other screening programs?

Answer. No, TSA has not.

SECURE FLIGHT AND PRIVACY

Question. Mr. Secretary, I'm concerned about reports from February and the end of March in which TSA officials, including a TSA spokesperson, declared that Secure Flight will be implemented in August with two airlines nationwide. That implementation would appear to violate the law as mandated by § 522 of the fiscal year 2005 Department of Homeland Security Appropriations Act that prohibits the spending of any sums appropriated on other than a test basis for Secure Flight unless and until the GAO certifies to Congress that 10 criteria are met. Is that implementation with two airlines scheduled to end at a certain time so that it can be evaluated?

Answer. TSA is proceeding with demonstrating initial operating capability for Secure Flight later this year. This timeframe is consistent with the requirements laid out in IRTPA. In addition, TSA intends to provide proof that each of the ten identified areas of concern and the six GAO recommendations have been addressed before the planned initial operating capability is implemented. Evaluations of the performance of the program with the launch carriers will be conducted prior to the program integrating additional airlines. A specific timeline is still under development to ensure that all appropriate evaluation takes place.

Question. Will the passengers flying those two airlines come late August be able to distinguish between a test run of Secure Flight and the real thing?

Answer. The passengers flying on the initial airlines will not be able to distinguish between the test run of Secure Flight and the "real thing." During the first phase of implementation, the carriers will continue their normal vetting activities and a parallel operations activity will be running in conjunction with TSA to confirm the effective processing of related data without disruption to ongoing business operations. Once the systems have performed in parallel for a period of time, and the acceptable stabilization has occurred, TSA will work with the carriers to ensure a smooth transition in taking over from them the full watch list vetting function.

Question. Do you anticipate that the Secure Flight program will, when finally implemented, use private companies to aggregate data on passengers and perform verification checks?

Answer. This is undetermined. TSA conducted a very limited test to determine whether the use of commercial data could improve the effectiveness of the watch list comparisons undertaken in the Secure Flight program as well as to assist with the identification of passenger information that is incorrect or inaccurate.

In the Homeland Security Appropriations Act, 2005 (Public Law 108–334, Section 522(d)), Congress mandated that prior to commercial data testing, TSA would be required to develop measures to assess the impact of using commercial data on aviation security, and that GAO is to review those measures. TSA is complying with all Congressional requests on this issue; GAO will continue to evaluate TSA's development of performance measures throughout the test phases. The limited commercial data testing concluded in July 2005.

TSA's testing of the use of commercial data is governed by strict privacy and data security protections, including strict prohibitions on the use of any passenger-provided information by commercial data providers. TSA will not incorporate the use of commercial data into Secure Flight unless testing confirms that:

—it enhances security;

—it does not result in inappropriate differences in treatment of any category of persons; and

—robust data security safeguards and privacy protections can be put in place to ensure that commercial entities do not gain inappropriate access to or use passenger personal information inappropriately.

TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Results of the testing, both of the comparisons of PNR information against names in the Terrorist Screening Database and the use of commercial data, will be as publicly transparent as possible without compromising national security. Testing and eventual implementation will be governed by strict privacy protections including passenger redress procedures, data security mechanisms, and limitations on use.

Question. How many companies could provide the data broker and data aggregation function to accomplish Secure Flight passenger verification?

Answer. This is undetermined at this point. TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Question. Will you examine whether the private companies bidding for this work have had data spills, or data breaches caused by identity thieves?

Answer. This is undetermined at this point. However, as with all contracts, TSA would set standards, establish program priorities and direction, establish policies, make program decisions, and monitor contractor performance. TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Question. What penalties will the Secretary impose on the company DHS and TSA eventually contracts with to perform passenger verification for Secure Flight if that company fails to properly safeguard data transferred as part of Secure Flight?

Answer. This is undetermined at this point. However, as with all contracts, TSA would set standards, establish program priorities and direction, establish policies, make program decisions, and monitor contractor performance. TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Question. I am concerned about recent GAO reports that show a lack of progress regarding establishing a transparent, concrete and workable system of due process and redress for passengers wrongly selected for extra scrutiny who might miss a flight and those who are wrongly put on a no fly list.

Mr. Secretary, please share with us what efforts you will take to ensure that the government's own watch lists and databases used for Secure Flight contain accurate information about would-be passengers.

Answer. U.S. Government intelligence and law enforcement agencies collect, analyze, and evaluate data used to nominate subjects to the No-Fly List. Intelligence analysts and law enforcement officers within these organizations carefully review nominations based on the No-Fly List criteria and thoroughly evaluate the information during each step of the process. Watch List nominations often contain classified and/or sensitive law enforcement investigative information. Nominations that meet the established criteria are forwarded to the National Counterterrorism Center (NCTC) and the Terrorist Screening Center (TSC) for inclusion in the TSC Data Base (TSDB) and for addition to the No-Fly List. Time sensitive nominations may be routed directly to the TSC if required.

If it is determined that a person on the No-Fly List should no longer be identified as a No-Fly subject, they will be removed from the list. If additional intelligence data is developed or a subject has been interviewed by U.S. Government officials and deemed no longer a threat, an official request for removal must be submitted to the agency that placed the individual on the list. The original nominating agency will evaluate the data and determine whether the person stays on or is removed from the No-Fly List. The nominating agency will then make a formal request through the nomination chain requesting that the person be removed from the No-Fly List. In some cases, a review of the derogatory information associated with a No-Fly nomination may result in the subject being downgraded to the TSA Selectee List.

The TSA Office of Transportation Security Redress is developing a redress process that will address any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening under the future Secure Flight program. This process will also allow passengers who feel they have been erroneously placed on the watch lists to undergo a case review. The Office of Transportation Security Redress will work to ensure that passengers erroneously placed on the watch lists are in fact provided relief. The redress process will be coordinated with other DHS redress processes as appropriate.

TSA has developed and implemented a clearance protocol for persons who are flagged for additional screening due to the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA will review the submission and reach a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. The Passenger Identify Verification Form, as well as other information, has been posted on TSA's public website at the following web address: http://www.tsa.gov/public/display?theme=157&content=09000519800fb8af

However, this clearance process will not remove a name from the watch lists. Instead, this process distinguishes legitimate passengers from persons who are on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Following TSA-required identity verification procedures, airline personnel can then quickly determine that these passengers are not the person of interest whose name is actually on the watch lists.

In addition, an individual may seek to challenge his or her inclusion on a watch list in a court of competent jurisdiction after the redress and appeals process within TSA has been exhausted.

Question. And tell us what concrete redress policies you envision for passengers wrongly detained for additional screening who might miss a flight or those wrongly placed on a no-fly list.

Answer. The TSA Office of Transportation Security Redress is developing a redress process that will address any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening under the future Secure Flight program. This process will also allow passengers who feel they have been erroneously placed on the watch lists to undergo a case review. TSA will work with the nominating agency to review the derogatory information. The redress process will be coordinated with other DHS redress processes as appropriate.

TSA has developed and implemented a clearance protocol for persons who are flagged for additional screening due the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA will review the submission and reach a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. The Passenger Identify Verification Form, as well as other information, has been posted on TSA's public website at the following web address: http://www.tsa.gov/public/display?theme=157&content=09000519800fb8af

It is important to keep in mind that this clearance process will not remove a name from the watch lists. Instead, this process distinguishes passengers from persons who are in fact on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Airline personnel can then more quickly determine when implementing TSA-required identity verification procedures that these passengers are not the person of interest whose name is actually on the watch lists.

In addition, an individual may seek to challenge his or her inclusion on a watch list in a court of competent jurisdiction, after the redress and appeals process within TSA has been exhausted.

US VISIT: WHEN WILL WE HAVE A REAL "EXIT" COMPONENT?

Question. The former DHS Under Secretary, Asa Hutchison, announced with great fanfare meeting the December 31, 2004 deadline to have the foreign visitor visa entry-exit system, known as US VISIT, up and running at the 50 largest land-border ports of entry. This is a positive accomplishment and I am pleased that the Department has taken seriously our mutual interest in knowing who is entering this country and in keeping out those who should not be allowed entrance.

However, I remain concerned that very few taxpayers know that while we may know who is entering the United States at our airports, seaports, and some land border ports, we continue NOT to know who is exiting the United States. That's right—there is almost no "exit' component to the US VISIT system—a system which used to be called "entry-exit". We have spent hundreds of millions of dollars on this system—and another $390 million is requested for US VISIT in the President's fiscal year 2006 budget, and yet we still are not able to capture data on which visitors are exiting the country.

How can we know if someone has overstayed their permitted time in this country if we do not know that they have left?

Answer. US VISIT is exploring different departure confirmation alternatives where biometrics are collected on exit, in addition to the biographic information, at 12 air and 2 sea port pilot locations. After evaluating these exit procedures, DHS will select the most effective process(es) and technologies to implement at airports and seaports nation-wide.

Currently the US VISIT system collects both biographic and biometric data on eligible (nonimmigrant) alien arrivals and departures and stores the data in the Arrival Departure Information System (ADIS).

—Biographic data is primarily collected through the submission of passenger manifests by the transportation carriers, with additional arrival and departure information collected by officers at U.S. ports-of-entry.
—Biometric data (digital fingerscans and photographs) are collected at consular posts during visa interviews, at U.S. air and sea ports-of-entry during admission, and at a limited number of pilot locations at air and sea ports during departure.
—US VISIT analyzes the data in ADIS to prepare the Annual Report on Integrated Entry and Exit Data System, as required by the Data Management Improvement Act of 2000 (Public Law 106–215) and the Visa Waiver Permanent Program Act (Public Law 106–396). The report is due on December 31 each year. The report for 2004 was transmitted to the Hill on August 19, 2005.
—During the last 3 months of the reporting period ending in September 2004, the system consistently matched 90 percent of exit records to entry records using biometrics due to the increased number of visitors enrolled in US VISIT at the

time of admission. The system successfully matched approximately 10 percent more exit records than when using biographic data alone.

—US VISIT then analyzes those remaining records to determine if stays were legally extended, there were approved changes in status, or information existing in other systems that would indicate that the individual did not overstay.

—Once US VISIT reviews all the information, those who are "confirmed overstays" are referred to ICE's Compliance Enforcement Unit for further vetting. Based on the outcome of its analysis, ICE may refer unresolved cases to the field for investigation. From January 2004 through August 2005, ICE has arrested almost 70 individuals based on overstay information provided by US VISIT.

—DHS also will leverage new technology in the land environment to capture information about and departures. Our first proof of concept using this new technology, radio frequency identification (RFID), began August 4, 2005, at three land border ports of entry along the Northern and two along the Southern borders. This technology can detect a visitor at a distance and provide primary inspection officers with entry information as well as provide a mechanism for an accurate and timely record of exits. The proof of concept testing at the ports of Nogales East and Nogales West in Arizona, Alexandria Bay in New York, and the Pacific Highway and Peace Arch in Washington will continue through 2006.

Question. What are the threats from not knowing who left?

Answer. These threats are difficult to measure. Where we develop a lead that someone is associated with a terrorist group after that person has entered the country ICE coordinates its investigative activity with necessary entities to take appropriate action. In addition, one of the purposes of the Immigration and Nationality Act (INA) is to exclude and remove criminals, terrorists, drug traffickers, and those who would work and live in United States illegally, from the United States. Individuals who overstay their visas contribute to the denigration of the integrity of our immigration system—that is why US VISIT works with ICE to locate and apprehend these immigration violators.

Question. When will we have a robust "exit" capability at our airports and at our land borders?

Answer. US VISIT is exploring different biometric departure confirmation alternatives at 12 airports and two seaports. The exit pilots require foreign visitors to check out at an exit station or with a US VISIT exit attendant at the departure gate at the port. After evaluating these exit procedures, DHS will select the most effective process(es) and technologies to implement at airports and seaports nationwide.

Question. How much more will this cost and when will this system be completed?

Answer. The fiscal year 2005 investment includes resources to modernize our immigration and border management systems and provide greater interoperability for immigration and border management data. In fiscal year 2005, we will increase interoperability technology and introduce basic common service-oriented architecture functionality to enable delivery of expanded person-centric view capabilities. We are currently developing the business requirements for the first phase of this strategy.

The fiscal year 2006 request includes resources to improve our immigration and border managements systems, as well as the continued deployment of US VISIT at our land borders. The fiscal year 2006 request includes operation and maintenance of current and 2005 investments, including: initial implementation of the entry and exit solution at air, sea and land ports of entry (POEs); implementation and integration of border technology to the busiest land POEs; and deployment of biometric travel document readers at air, sea, and land POEs.

US VISIT

Question. In the Immigration and Customs Enforcement (ICE) reprogramming request submitted to Congress on March 11, 2005, the Department offered up as a "bill payer" a portion of the US VISIT "management reserve." The US VISIT program office had vociferously advocated for this reserve. The Department suggested that this reserve could be reduced by $17 million to meet the ICE funding shortfalls which had been known by the Department for sometime.

Does this mean that the US VISIT management reserve is a lower priority to the Department? Will we see this reflected in the next US VISIT spend plan we expect to see regarding the fiscal year 2006 funds?

Answer. All components within DHS were asked to review their budgets to determine if they could help address ICE funding needs. Management reserve within US VISIT exists to address unforeseen funding issues as they arise. This helps reduce

program risk. Because of the nature of the purpose of management reserve, it is difficult to determine with certainty how much is needed in any given year. To reduce programmatic risk on ICE programs, it was appropriate to propose to accept temporary higher risk for US VISIT. However, a normal level of management reserve must be an integral part of the program into the future.

The recently enacted fiscal year 2005 supplemental for ICE eliminated the need to reprogram funding from US VISIT for this purpose.

TWIC PROGRAM—WHY THE DELAY?

Question. During his confirmation hearing before the Senate Homeland Security and Governmental Affairs Committee on March 8, 2005, then Deputy Secretary-nominee, Michael Jackson, said he did not understand why it was taking so long to get the Transportation Worker Identification Credential (TWIC) program up and running. He said, "It's not rocket science." A number of states, notably Florida, have already moved forward with their own credentialing programs for their State workers. Mr. Secretary, if this program is not "rocket science", what is causing the delay? Congress has provided upwards of $65 million towards the program, pilot projects are underway, and thousands of workers are waiting. Why the delay? Is this delay the result of resource-constraints, policy decisions, privacy protections (or lack of clarification of privacy protections) decisions, some combination all of these, or something else?

Answer. TSA acknowledges that the TWIC prototype has proceeded slower than expected. Technical and contractual issues have delayed rollout of the final TWIC card model and installation of final version biometric access control readers. Those issues are now solved. Enrollments and card production are ramping up at East and West Coast sites. The Florida rollout has been slowed as the State of Florida's team worked to resolve issues unique to Florida due to the need to comply fully with the Florida Uniform Port Access Credential (FUPAC) Act. Working with both State personnel and the prototype contractor the program has been successful in addressing and solving these problems. The ability to discover and resolve problems during the prototype phase rather than during implementation has been a welcome and valuable result and will benefit the program as it moves forward.

The TWIC Program achieved initial operating capability (IOC) for each region on November 17, 2004. IOC was defined as having functional enrollment capability and at least one operational TWIC reader at one or more sites within the region. Presently, TWIC is in Phase III-Prototype whereby TSA is evaluating a full range of business processes, policies and requirements for an end-to-end solution that includes sponsorship, claimed identity verification, criminal history records checks (in the State of FL only) and card production, personalization, and issuance as well as revocation. Once Phase III-Prototype is complete, TSA will conduct further analysis and make recommendations regarding the nature and scope of Phase IV-Implementation.

EXPEDITED TRAVELER EXPANDING OVERSEAS

Question. The Department announced the creation of pilot expedited traveler program at Schipol Airport in Amsterdam, yet there has been no decision made on expanding or making permanent the limited pilot tests of the Registered Traveler program here in the United States. Why is there a delay with expanding the domestic Registered Traveler program?

Answer. While both programs enhance the security of civilian aviation, the two programs serve different purposes. The International Register Traveler Program is intended to enhance the already-existing requirement that CBP inspect and interview travelers seeking to enter the United States, and the program enhances CBP's ability to make admissibility decisions by separating out low-risk travelers. It builds on legacy trusted traveler programs—e.g., SENTRI, NEXUS, FAST, INS PASS. The domestic registered traveler program, by contrast, is a pilot program to improve the aviation security screening process by helping TSA align screeners and resources with potential risks.

Through a series of concurrent stand-alone pilots, TSA has been aggressively testing the Registered Traveler (RT) concept of running threat assessment and identity verification checks on eligible volunteers in order to provide them with an expedited clearance through security checkpoints. TSA is currently running pilot programs at five Federally managed sites (Minneapolis, Los Angeles, Houston, Boston, and Washington, D.C.), which are scheduled to be completed in September 2005. TSA has also worked with the Greater Orlando Aviation Authority (GOAA) to launch a pilot at Orlando International Airport that is assessing the feasibility of incorporating a private sector component into the RT concept.

Results of these pilots will be analyzed to determine the program's effect on security and service, enabling the Department to make decisions about full scale implementation of RT. Any timeline and deployment schedule for implementing RT beyond the pilot stage will be linked to the Department's decision.

Question. If we're not sure the domestic program is going to work—or how exactly it should be structured—why are you starting an international version at this time?

Answer. While both programs enhance the security of civilian aviation, the two programs serve different purposes. The International Register Traveler Program is intended to enhance the already-existing requirement that CBP inspect and interview travelers seeking to enter the United States, and the program enhances CBP's ability to make admissibility decisions by separating out low-risk travelers. It builds on legacy trusted traveler programs—e.g., SENTRI, NEXUS, FAST, INS PASS. The domestic registered traveler program, by contrast, is a pilot program to improve the aviation security screening process by helping TSA align screeners and resources with potential risks.

Through a series of concurrent stand-alone pilots, TSA has been aggressively testing the Registered Traveler (RT) concept of running threat assessment and identity verification checks on eligible volunteers in order to provide them with an expedited clearance through security checkpoints. TSA has run pilot programs at five Federally managed sites (Minneapolis, Los Angeles, Houston, Boston, and Washington, D.C.), which are scheduled to be completed in September 2005. TSA has also worked with the Greater Orlando Aviation Authority (GOAA) to launch a pilot at Orlando International Airport that is assessing the feasibility of incorporating a private sector component into the RT concept.

Results of these pilots are being analyzed to determine the program's effect on security and service, enabling the Department to make decisions about full scale implementation of RT. Any timeline and deployment schedule for implementing RT beyond the pilot stage will be linked to the Department's decision.

LACK OF FUNDING FOR BORDER SECURITY

Question. During the hearing, you stated that the President's budget for fiscal year 2006 both hires 210 new Border Patrol agents, hires more immigration investigators and provides 1,920 new detention bed spaces and, at the same time, provides sufficient funds to backfill and hire the positions that were lost during the current fiscal year.

Are you guaranteeing that the budget request hires both all fiscal year 2005 attrited Border Patrol positions and 210 new Border Patrol agents?

Answer. The fiscal year 2005 Emergency Supplemental provides funding for 500 additional Border Patrol agents. CBP has until the end of fiscal year 2006 to fill these positions. However, CBP plans to hire these positions aggressively. For fiscal year 2005, CBP will backfill its fiscal year 2005 attrited positions and hire approximately 400 (of the 500) additional agents.

For fiscal year 2006, the President's Budget requests 210 additional Border Patrol agents. Both House and Senate Appropriations bills add 790 Border Patrol agents on top of this (for a total of 1,000). If enacted, CBP would hire these positions and backfill estimated attrition (approximately 600 positions).

With that said, the total impact of the fiscal year 2005 Supplemental and the anticipated fiscal year 2006 budget will result in 1,500 new Border Patrol agents by the end of fiscal year 2006. CBP will also hire for the backfill of attrition. CBP has the capacity to hire and train this level.

With respect to ICE, the fiscal year 2006 President's Budget, when combined with projected carryover balances from the fiscal year 2005 Emergency Supplemental, contains sufficient funding to support 376 fiscal year 2005 attrition hires. In addition, the fiscal year 2006 President's Budget includes an increase of $90 million to support 1,920 beds.

Question. And at what point in fiscal year 2006 will the Border Patrol have hired and trained the same staffing level at the start of fiscal year 2005 positions, plus the 210 new agents?

Answer. CBP ended fiscal year 2004 with 10,817 Border Patrol (BP) agents. For fiscal year 2005, CBP plans to maintain that staffing level as well as beginning to add the 500 new agent positions provided in the fiscal year 2005 supplemental. For fiscal year 2006, CBP plans to add the 210 new agents in the President's Budget and replace all attrition positions. Hiring for the additional BP agents is a high priority.

BORDER SECURITY

Question. The Heritage Foundation's December 13, 2004 report recommends that the Department "conduct a national assessment of the resources required for effective border security." Is this recommendation a part of your comprehensive review of the Department and its priorities?

Answer. The Department has been working aggressively outside of the Second Stage Review process to assess our long-term border needs, including the resources needed to secure substantial improvement in control of our borders. Complimentary Second Stage Review efforts examined needs in such areas as cargo security and passenger screening. The Department also is developing a plan for an independent, outside entity to examine border resource needs. All of our efforts will coalesce into the development of a long-term border security and immigration reform plan.

IMPACT OF REAL ID ON BACKLOG REDUCTION/WORKLOAD

Question. The House attached Rep. Sensenbrenner's REAL ID immigration bill (H.R. 418) to the Emergency Iraqi War Supplemental. This bill includes many of the provisions in the original House draft of the Intelligence Reform and Terrorism Prevention Act.

Unlike some rhetorical Bush Administration amnesty, the specifics of this legislation are known. The Administration supports the REAL ID legislation.

If the conferees decide to include the provisions of this bill in the Supplemental, what impact would it have on Citizenship and Immigration Service's abilities to meet its backlog reduction goals and what resources would be required to implement the Act?

Answer. Based upon our review, the Real ID legislation should have no impact on the backlog elimination plan. The additional fee revenues as a result of this legislation ensure the timely processing of these cases.

The verification and adjudications functions of USCIS are organizationally separate. The verification workload is handled by Immigration Status Verifiers (ISVs) in the USCIS Records program, who are dedicated and specially trained for that function. USCIS does not intend to divert adjudications resources to implement the REAL ID Act. Therefore, backlog elimination goals will not be impacted.

PASSPORT PRIVACY

Question. As the State Department is looking into the issue of possibly embedding personal data in the next generation of U.S. passports, what if any discussion has the Department's Privacy Officer had with State Department officials about the protection of the privacy of U.S. citizens?

Answer. The Chief Privacy Officer for DHS has a very good working relationship with officials from the Department of State on matters of mutual concern, including lost and stolen passports and appropriate privacy notices for international travelers. While the Privacy Officer has made her views known to the State Department on numerous privacy matters, the precise question of how to protect personal information in the next generation of U.S. passports is one that is being worked on primarily by the Department of State, which has the lead authority for matters pertaining to passports. Of course, the DHS Chief Privacy Officer will work collaboratively with the State Department to ensure that implementation of any decisions protect the privacy of U.S. citizen's information.

CARGO CONTAINER SECURITY

Question. The conference report accompanying the fiscal year 2005 Appropriations Act notes that over $200 million has been spent over the past 3 years on various projects designed to secure cargo containers entering this country. It also calls on the Under Secretary for Border and Transportation Security to report to the Congress no later than February 8, 2005 on which DHS entity will have primary responsibility for cargo container security and the setting of shipping industry standards. To date we have not yet received that report. When can we expect to see it?

Answer. This report was submitted to Congress on May 31, 2005.

Question. Are funds included in the President's budget request to achieve this goal?

Answer. The President's fiscal year 2006 Budget includes $138 million for the Container Security Program.

SUPPLY CHAIN AND CONTAINER SECURITY

Question. We received part one of the Supply Chain and Container Security report required by House Report 108–541. It states that the Container Security Initiative

Division in headquarters "is staffed with a majority of CBP employees and a small number of ICE Special Agents.

Please provide the total number of the CSI Division headquarters staff and the number of those who are ICE Special Agents. Also, at which—if any—of the overseas CSI ports do we have both an ICE and a CBP attaché?

Answer. The Container Security Initiative (CSI) Division headquarters staff consists of 52 full time employees, four of which are ICE Special Agents. At this time, there are no CSI ports with both an ICE and a CBP Attaché.

MERGING CBP AND ICE

Question. You currently are conducting a "top to bottom" review of the Department, its structure, and its operations. Recent reports, including a December 13, 2004 Heritage Foundation report, bemoan the artificial division of Customs and immigration inspectors from Customs and immigration agents and recommend that CBP and ICE be merged. What is the status of the Department's discussion on these recommendations? When will the Congress learn of your intentions, if any, in this regard?

Answer. We are not merging ICE and CBP; however, we do see the need to ensure that these organizations coordinate better. We will continue to work closely with the leaders of ICE and CBP to improve cooperation and coordination between these agencies. In deciding to not merge the two agencies, we considered view points from a variety of sources, including think tanks, as well as the Department's Inspector General, Members of Congress, and other valuable stakeholders.

As you know, the Department looked at a variety of organizational issues as part of the Second-Stage Review process, which helped clarify where the Department needs to be organizationally to ensure effective implementation of our critical missions. We considered whether ICE should remain a stand-alone entity, and decided that it should. We believe it's in the Department's best near and long-term interest that ICE not be merged with another component, CBP in particular. To reach this decision, we focused on the operational mission needs of both CBP and ICE, not on the near-term management challenges. I take seriously the challenges the Department has faced concerning ICE and appreciate the difficult but necessary choices Congress has made in providing new funding to address its needs. I am confident, however, that ICE has made substantial improvements in financial management this year. Not only have substantial new resources been provided, but a new management team is taking shape.

IDENT/IAFIS

Question. The integration of the fingerprint databases created, maintained, and used by the Department of Homeland Security and the FBI—among other Federal agencies—continues to be a priority concern for the Congress and the members of this Subcommittee. Border Patrol agents daily compare the fingerprints of illegal aliens apprehended at our borders against these databases. And Customs and Border Protection inspectors—at a growing number of ports of entry—compare the fingerprints of visa holders and others wishing to enter this country against these same databases via the US VISIT system.

That is why I was concerned about the latest Department of Justice Inspector General report on this subject. It stated that of the 118,000 visitors daily entering this country who are subject to US VISIT, an average of about 22,350 individuals are referred for secondary inspection.

According to DHS, by the end of this fiscal year, it expects to directly check only about 800 individuals each day against the full FBI fingerprint database known as the IAFIS Criminal Master File. This is just 0.7 percent of the 118,000 daily visitors. The vast majority of the visitors, 99.3 percent, will be checked only against the US VISIT watch list. These persons will not be checked directly against the full IAFIS Criminal Master File. Why is that the case? Why are so few people being run against these valuable investigative tools?

Answer. The Department continues to work closely with the Department of Justice to improve the integration and interoperability of our fingerprint databases and we have established an integrated project team. Currently, the FBI updates DHS' records with information from a variety of criminal and threat-related databases. Based on updates to the US VISIT system during the time period between January 2004 and the end of August 2005, officers have taken adverse action against more than 800 individuals during US VISIT processing on entry. In addition, integrated DHS Automated Biometric Identification System (IDENT) and FBI Integrated Automated Fingerprint Identification System (IAFIS) workstations will be deployed to all POEs with significant passenger volume, as well as to ICE locations by the end of

calendar year 2005. A report, describing plans for interoperability, was submitted to Congress on August 18, 2005.

On July 13, 2005, I announced a decision that first-time visitors to the United States will be enrolled in the program by submitting ten fingerscans—a key step to achieving interoperability between IDENT/IAFIS. We have worked with the Departments of State and Justice to develop an implementation plan for the Initial Transition to 10 Print Plan which addresses interoperability as well as migration to 10 fingerscans. In addition, the capability to capture 10 fingerscans will allow us to increase accuracy for matching individuals against watch lists and previous enrollment records; improve DHS's ability to match enrollees against latent prints; and allow DHS to focus more time and attention on individuals who might be potential risks to the country.

Question. The Conference Report accompanying the fiscal year 2005 Homeland Security Appropriations Act directs the Department to fund the full cost associated to achieve real time interoperability with the US VISIT system. Yet there does not appear to be any funding in the budget to either establish real time interoperability of the DHS and Justice fingerprint databases, or an expansion of the current DHS system of capturing 2-fingerprints versus movement towards a 10-print system.

Why is there no specific funding in the budget to improve the interoperability of IDENT/IAFIS and US VISIT?

Answer. On July 13, 2005, I announced a decision that visitors to the United States will be enrolled in the US VISIT program by submitting 10 fingerscans. DHS is working with the Departments of State and Justice to develop an implementation plan that will address interoperability as well as migration to 10 fingerscans and cost estimates.

There are several different ongoing efforts to bring about interoperability between the IDENT/IAFIS systems. Integrated IDENT/IAFIS capabilities were deployed to all Border Patrol stations ahead of schedule in fiscal year 2004 and additional deployment to all POEs with significant passenger volume and ICE offices will be completed by the end of calendar year 2005. The US VISIT program will use $9.3 million of fiscal year 2005 resources to complete the deployment of IDENT/IAFIS access configuration at 115 airports, 15 seaports, and 165 land border POEs, as well as to specific ICE locations.

The fiscal year 2006 budget request includes resources for improved interoperability and the integrated project team will develop cost estimates for primary integration and development associated with IDENT/IAFIS interoperability as it develops its plan.

IDENT/IAFIS INTEGRATION

Question. In the Department's "2004 Year End Review", it is noted that the Integrated Automated Fingerprint System (IAFIS) was operational at all Border Patrol stations 3 months ahead of schedule. This is a positive first step. However, nowhere in the report does the Department discuss the progress at fully integrating the IAFIS and IDENT fingerprint databases. The statement of managers accompanying the conference report on the fiscal year 2005 Appropriations Act discusses at length the strong congressional interest having these databases fully integrated. In fact, this was a topic that generated much bipartisan discussion during one of our hearings last year. Chairman Gregg again stressed its importance during our hearing with you this year.

Integration has also been the subject of at least three Department of Justice inspector general reports.

Who in the Department has the lead on this subject?

Answer. The US VISIT Program, working closely with DHS components such as CBP and ICE, and the Departments of Justice and State, leads the efforts for full IDENT/IAFIS interoperability within the Department.

Question. What is the timeline for accomplishing this integration and how much will it cost?

Answer. DHS (US VISIT) and FBI/CJIS have established an IPT to address the policy, business requirements, and technical aspects of integrating IDENT and IAFIS. This IPT has made significant progress in resolving many of the long-standing issues originally referenced by the DOJ Office of the Inspector General. A report, describing plans for interoperability, was submitted to Congress on August 18, 2005.

Question. Are sufficient/any funds included in the President's budget request for this activity?

Answer. The Departments of Homeland Security and Justice will develop future budgets to support any necessary level of funding for IDENT/IAFIS interoperability.

VEHICLE FLEET MANAGEMENT REPORT

Question. Senate Report 108–280 required the submission by February 8, 2005 of a vehicle fleet management report. That report has yet to be submitted. It is difficult for the Congress to provide funds for new and replacement vehicles when we have little confidence that decisions to purchase these vehicles are being made in a methodical and reasoned manner. When can we expect to receive this overdue report? Also, please break out by type/category of vehicle the funds requested in the budget for new and replacement vehicles for the various CBP entities.

Answer. The requested report is now being reviewed and will be submitted to Congress as soon as possible. The type and number of vehicles to be purchased will be based on the operational priorities of the Border Patrol in fiscal year 2006.

AMO FLEET MODERNIZATION PLAN

Question. House Report 108–541 required submission of a report on the costs and benefits associated with a service life extension program of the P–3 Orion aircraft 30 days after enactment of the act. To date we have not received this report. Please provide us with this report as well as the status of Air and Marine Operations long-term procurement plan for new and replacement air and marine assets, including P–3.

Answer. A technical and operational review of responses received in reply to the CBP Request for Information (RFI) issued on February 28, 2005, has been completed. This review concluded that while there are viable alternatives to either replace or remanufacture the CBP/AMO P–3 fleet, this effort should be part of a formal acquisition process associated with CBP/AMO's overall modernization initiative. CBP's long-term modernization plan will be developed as a component of the CBP air asset integration study to be completed in the summer of fiscal year 2005.

APHIS—FOOD SAFETY INSPECTORS

Question. Since the announcement of the creation of the Department, I have been concerned that "core" missions of the various legacy agencies would get lost because of the new Department's primary focus on homeland security. One area of concern is agriculture inspection operations at our borders.

Border inspection responsibilities, including 2,500 frontline inspectors, were transferred from the Animal and Plant Health Inspection Service (APHIS) to DHS in March of 2003.

According to a recent U.S. Department of Agriculture Inspector General report, APHIS could not assure that the DHS process for agriculture inspection operations contains adequate controls to safeguard U.S. Agriculture against entry of foreign pests and disease. It also noted that there was a reported 32 percent drop in the number of pest inspections following the transfer to DHS. What is the Department doing to correct this?

Answer. The effort to bring up the number of CBP agricultural specialists to the level transferred from APHIS is a priority and CBP has made significant progress. According to the Determination Order that actually transferred personnel from APHIS, 1,872 agricultural specialists including canine were sent to DHS CBP. Of these positions, 316 were vacancies. In fiscal year 2005, the hiring of additional Agriculture Specialists is a priority. The USDA Professional Development Center (PDC), the APHIS entity responsible for training new CBP agricultural specialists, has scheduled 20 classes from May 2004 through February 2006. Seven classes have graduated as of April 22, 2005, with 203 graduates deployed to 62 POEs. It is projected that CBP will have 500 graduates by February 2006.

In addition to training more agricultural specialists, under CBP's "One Face at the Border" initiative, all CBP Officers at the POEs are used to perform the vast number of functions that CBP is charged with carrying out. In terms of agricultural inspections, CBP officers are being cross-trained, learning basic agriculture procedures for the land border, mail, cargo, maritime, and air passenger pathways to increase the value of referrals and supplement the work of the Agriculture specialists.

CBP has noticed that several positive developments have resulted in a greater level of compliance in agricultural importations. Offshore mitigation strategies by APHIS to minimize the number of pests even reaching the United States are working. CBP, in conjunction with APHIS, has entered into several programs, such as a targeted program for imported cut flowers that decreased the number of inspections because the scientific data indicates that such commodities pose a much lower risk to American agriculture. During the same period, interceptions of prohibited animal by-products went up by 26 percent and prohibited meat and poultry by 6 percent.

In summary, as the vacancies are filled with newly trained specialists, CBP will create a sufficient workforce of agricultural specialists to target and intercept prohibited material, and report all insects found in CBP seizures. When this occurs, the interception rate will more precisely reflect the true level of CBP efforts. CBP has asked USDA to supply additional insect pest detection training at POEs based on the specific pest pathways of concern.

Question. Is the Department working with APHIS to establish a method to coordinate information regarding inspections?

Answer. DHS–CBP has been working with and coordinating with USDA–APHIS in numerous ways to synchronize and verify information and data collected about inspections. The following are some of the ways CBP and APHIS have worked together.

Joint Quality Assurance (QA) Program

—CBP and APHIS have formed a joint QA team and began conducting port reviews together.
—QA reviews will assist the Directors, Field Operations and improve our credibility among agricultural stakeholders.
—CBP's Agricultural Inspections Policy and Programs (AIPP) conducted successful Joint APHIS QA reviews at the Port of Philadelphia, December 7 and 8, 2004, and the Port of Miami, April 18–22, 2005.
—Plans and dates are being developed to conduct Joint QA reviews once a month for the remainder of fiscal year 2005.
—The QA team produces recommendations that are conveyed to CBP management for consideration and action.

Creation of selectivity criteria and rule sets for agricultural targeting

—CBP AIPP and APHIS are working together to develop rule sets for targeting and prevention of Agro/Bio Terrorism.
—Plans are in place to hire two CBP Agriculture Specialists to be assigned to the National Targeting Center (NTC).
—CBP assisted APHIS in the placement of one employee at the NTC to target and help prevent Agro/Bio Terrorism.
—CBP has engaged and included APHIS in discussions about developing selectivity criteria for agricultural products.

USDA access to CBP databases

—CBP has been instrumental in negotiating an agreement with USDA to share data and databases between the agencies.
—CBP has granted access for certain USDA offices to relevant CBP databases.
—The combination of USDA databases and CBP databases and electronic systems will add to our capability to measure agricultural risk worldwide, target, develop new rule sets, and build CBP's expertise and capacity for early threat detection.

Communications within CBP

—CBP is making efforts to redesign and improve the Agriculture Inspection section of the cbp.gov website to be an effective means of communication within CBP.
—The intranet site, cbp.net, is being redesigned to highlight joint actions and important efforts with USDA/APHIS.
—CBP uses a system of alerts and musters as well as other CBP systems to notify the ports of issues of immediate concern.

Joint Operations with USDA—Measurement Driven Special Operations (MDSO)

—Fifty joint MDSO's are proposed for the remainder of fiscal year 2005.

Management Inspection Division (MID)

—CBP used the MID to establish audit protocols that target mission critical agriculture functions.
—Planning inspections at JFK, Miami, Los Angles and Newark International Airports: International Mail, Pest Interceptions (Cargo), Pest Interceptions (PAX), Cargo Control (Agriculture), Agriculture Quarantine Inspection Monitoring (AQIM).
—Proposed MID Inspections at Port Elizabeth, Baltimore, and Buffalo: AQIM.
—Proposed MID Inspections Nogales, El Paso, Blaine, and Puerto Rico: AQIM.

Self-Inspection Reporting System (SIRS)

—CBP AIPP also uses the SIRS to monitor the agricultural program and to identify areas for improvement.

—CBP AIPP has developed self-inspection worksheets based on Office of Field Operations (AIPP) policies based on USDA regulations, rules, policies, and needs.
—For example, worksheets target Data Management, Cargo Control, Pest Exclusion, International Mail, and Clearance of Conveyances.

Question. The report claims that the Department has denied APHIS access to port locations when access was requested, even to perform duties for which APHIS still has regulatory responsibility. Is this true and, if so, why was this access denied?

Answer. CBP and USDA–APHIS have forged a new working relationship and resolved many of the earlier port access issues. CBP and USDA employees are working together cooperatively and sharing resources. CBP has worked with USDA to achieve the appropriate level of access to the POEs for their personnel. As Congress has provided, the inspectional functions were transferred from USDA to CBP. CBP has set forth procedures that have facilitated USDA gaining access to the ports to perform their functions.

CBP and USDA–APHIS signed in February 2005 Appendix 8 to Article 8 of the Memorandum of Agreement (MOA) between DHS and the USDA. The MOA establishes and enhances coordinated actions and operations between the two agencies and responds to many of the issues raised in the OIG report.

Question. The report also states that APHIS and the Food Safety and Inspection Service (FSIS) do not require DHS to notify FSIS of all incoming shipments, which could allow the shipments to bypass FSIS re-inspection. Is this correct and, if so, why?

Answer. DHS and USDA are currently developing a MOA to address the data needs of the Food Safety and Inspection Service (FSIS) as well as other USDA agencies.

In conjunction with FSIS, CBP has developed rule sets within our targeting systems to assist with the notification process. CBP and FSIS meet once a week to discuss food safety issues and FSIS has assigned an employee to work at CBP 2 days a week as a liaison. CBP is working very closely with FSIS to make sure that they are properly notified about arriving meat shipments. USDA and FSIS are also working together to update USDA manuals that would require notification of such shipments to FSIS.

Question. Has the Department provided adequate data on staffing levels and deployment of agriculture inspectors to APHIS for evaluation?

Answer. We are unaware of any formal APHIS request for such information nor what type of evaluation is contemplated by the question. However, CBP shares data concerning staffing levels and deployment of CBP agriculture inspection personnel with APHIS regarding training needs for newly hired CBP agriculture specialists in cooperation with CBP and is thus aware of the numbers of new hires.

CBP and APHIS also conduct joint QA port reviews that explore staffing as a standard element. APHIS has identifiers and other personnel at the ports that can verify the staffing levels.

PULSED FAST NEUTRON ANALYSIS

Question. On April 13, 2005, my staff received a report regarding the PFNA program called for by House Report 108–280. This overdue, four paragraph report stated that the contractor testing of this program, which was supposed to have begun in June 2004, been completed by October 2004, with a report issued by December 2004, has "set a firm date of April 18, 2005, for the test to begin." That date has now passed. Did the test start on April 18, 2005? If not, when did or will the test begin? Can you confirm that "the testing will be completed by August 19, 2005, and (that) the test report should reach Congress by November 2005"?

Answer. The operational evaluation of the Pulsed Fast Neutron technology commenced on May 2, 2005, and is scheduled to run for 4 months. An evaluation of the test is expected to be issued in November 2005.

USE OF UNMANNED AERIAL VEHICLES

Question. I understand that the Department has issued a Request for Information to private industry to determine the capability and availability of Unmanned Aerial Vehicle (UAV) systems for use in border control and enforcement. What is the deadline for industry response?

Answer. The RFI for the UAVs was issued on April 13, 2005, and responses were due on April 29, 2005. CBP received 14 responses.

Question. Have you engaged in a dialogue with the private sector about your needs and requirements in this area?

Answer. As noted above, CBP initiated dialogue with the private sector on UAV capabilities and CBP performance requirements through the RFI.

Question. Do you plan to engage in down select and fly-off between competing systems?

Answer. We do not plan to engage in fly-offs between competing systems during down select for the following reasons: the time constraint to establish an Initial Operating Capability (IOC) in fiscal year 2005 does not allow for this, market research resulted in a decision to procure mature commercial off the shelf technology, the development of a refined CBP UAV Performance Specification clearly outlines system requirements, and the RFI included the CBP Performance Specification.

Question. When do you expect a Request for Proposal to come forward and what is the target date to begin acquisition of a system?

Answer. CBP released a Pre-solicitation notice on May 10, 2005, that was followed by an RFP on June 21, 2005, which closed on July 20, 2005. CBP is in the process of evaluating proposals and anticipates a contract award on or about August 29, 2005.

Question. During the period June through September, 2004, there was a pilot program that successfully demonstrated the value of UAVs under the Arizona Border Control Initiative. What were the results of that demonstration and will the lessons learned be incorporated into the Department's long-term acquisition strategy?

Answer. The pilot program demonstrated that the UAVs had some operational effectiveness, but will require further evaluation to determine its optimal deployment. Some of the evaluation criteria were incorporated into the Request for Proposals issued for the purchase of UAVs for CBP. Lessons learned have been incorporated into both the present and long-term DHS acquisition strategies.

Question. I understand that one of the lessons learned from last summer's pilot program was that the initial speed to "get something flying" resulted in some inefficiencies in operation of the system (such as the location of where it was operated and the limited hours it was able to fly) which might have been avoided with proper planning. Are things like this being taken into consideration as you move forward with the program?

Answer. Yes, the lessons learned from the pilot program are being considered as we move forward with the present acquisition. Much attention is being focused on system acquisition, operational procedures and UAV basing to afford DHS the best solution to effectively meet our requirements.

Question. In view of the continuing flood of illegal aliens across the Southwestern Border and the reported success demonstrated with the 2004 UAV program, why hasn't the Department used the $10 million Congress appropriated for UAVs in fiscal year 2005 to restart the demonstration program as an effective enforcement and learning tool while the long term UAV program is developed?

Answer. The Department has evaluated the lessons learned from the two prior UAV deployments and has established UAV requirements that, although mindful of other DHS users, meet CBP's specific needs. A request for proposals was issued in June 2005, and follows the request for information that closed on April 29th. The $10 million in fiscal year 2005 is to be used for a UAV acquisition and subsequent deployment of a UAV system that will serve as the DHS UAV initial operating capability along the Southern border this fiscal year. In the interim, CBP has deployed a Cessna 206 and two Piper Cheyenne airplanes (all equipped with electro optical and infrared sensors) to the Arizona desert to adequately provide aerial surveillance until CBP can acquire and field its own UAVs.

As noted above, DHS is in the midst of a systems-level review of its border control architecture to identify the right mix of personnel, technology and infrastructure to help achieve effective control of the border.

Question. If it chose to do so, how soon could the Department restart that demonstration?

Answer. Since all necessary support requests have since expired, CBP would have to re-negotiate Letters of Procedure with all other airspace managers, a Request for Assistance from the Department of Defense (DOD) to allow us the use of Ft. Huachuca's facilities and logistics, and a Certificate of Authorization issued by the Federal Aviation Administration (FAA) to allow UAVs to operate in the National Airspace System. The earliest the demonstration could be restarted is 60 days from deciding to do so.

DHS "BRANDING" NOT COMPLETED

Question. The Department claims great success with some of its systems integration, including that of its legacy e-mail systems. However, my staff was surprised to learn that one legacy agency—the Federal Protective Service (which transferred over in its entirety from the General Services Administration)—still uses "gsa.gov" for its e-mails as opposed to the DHS "branded" "dhs.gov". What is most troubling

is that the FPS must continue to pay GSA for its e-mail services while also being billed by DHS (or ICE) for these same services—which it is not receiving. Why is there a delay in fully integrating FPS into the Department's operations?

Answer. Fiscal year 2005 resources were committed early in the year to expedite the conversion, which was over 80 percent complete as of March 31, 2005. The remaining Federal Protective Service (FPS) locations were converted by August 19, 2005.

Question. How much has FPS had to pay to GSA for this service this fiscal year to date?

Answer. Fiscal year 2005 GSA charges for FPS information technology support through August 1, 2005, totaled $5,837,498. All FPS offices with the exception of FPS HQ have been converted to the DHS Network. FPS Headquarters is scheduled to relocate from GSA (18th/F) to ICE Headquarters as of August 22, 2005. FPS will reimburse ICE OCIO for services provided.

Question. Since the Department has made claims that all agencies are on the same e-mail system, will the FPS be "made whole" or otherwise reimbursed as a result of these double payments?

Answer. The FPS will fund conversion costs to the DHS email system. FPS has not made, nor will it make, double payments.

C–TPAT

Question. In your statement for the record you say that C–TPAT is due for an increase of $8.2 million and that these funds "will be used to enhance our ability to conduct additional supply chain security validations." Is that the sole purpose for the increase, or will the program also be expanded with these funds?

Answer. CBP intends to use these funds to support the validation process.

Staffing for this program was significantly increased in fiscal year 2005 (120 new positions provided for conducting validations), which will allow CBP to conduct validations of all high-risk supply chains. An aggressive hiring drive to recruit permanent Supply Chain Specialists (SCSs) is underway, and CBP anticipates having 100 permanent SCSs on board at the end of fiscal year 2005. Additionally, CBP has trained 38 field officers to help with the initiation of validations.

As of August 15, 2005, the C–TPAT program has completed validations of 16 percent of certified members, and has validations underway on another 36 percent of certified members.

As of August 15, 2005, the C–TPAT program has over 9,700 applicants, of which 5,174 have been accepted and are certified. With an average of 2,000 to 3,000 new applicants each year, C–TPAT anticipates continued program growth and expansion through fiscal year 2006 and beyond.

Question. Please describe the "security validations" that will be conducted with the proposed increase.

Answer. Validations begin with a domestic corporate meeting. Foreign site visits typically include a corporate meeting with foreign manufacturer corporate personnel, and a tour of appropriate manufacturing, shipping/consolidation and port facilities. Validations conclude with a close out meeting between CBP SCSs and the certified member's Point(s) of Contact(s). The Validation Report issued by the CBP SCS contains sections on Findings, Recommendations and Best Practices.

CBP initiates validations based on risk, using a quantitative risk assessment tool to identify certified members with high-risk supply chains. CBP uses a validation selection methodology that relies upon quantifiable data coupled with an objective assessment of the submitted security profile to determine the top priorities for validations. Validation resources are then directed accordingly.

CBP uses a risk-based approach to validate the security enhancements that have been committed to by C–TPAT members, to evaluate the status and effectiveness of key security measures in the participant's profile, and make recommendations where appropriate. In particular, CBP is placing emphasis on the importer and carrier sectors, and has modified its validation approach to maximize resources and increase efficiencies, such as validating multiple foreign suppliers within a geographic proximity.

Moreover, CBP has enhanced its ability to record and measure validation results by developing the Automated Validation Assessment Tool, which is an electronic questionnaire that automatically scores and weighs the findings of the Supply Chain Specialist to produce an overall assessment of the supply chain security measures in place. Any identified weaknesses must be corrected in order to retain program benefits.

Once the Validation is completed, the C–TPAT partner's role in the process continues as follows:

—Communication on supply chain security issues continues with CBP and the assigned SCS;
—Continual self-assessments of supply chain and security processes and procedures are performed;
—A pro-active approach is maintained with regard to supply chain security and membership in C–TPAT.

ILLEGAL IMMIGRATION

Question. I am concerned that illegal immigrants continue to find new ways into this country. I understand that since the Navy stopped training and steaming in Vieques, Puerto Rico that there has been a surge of illegal immigrants coming to the United States through the Eastern Caribbean into Puerto Rico. What are you doing to close this gap?

Answer. CBP arrest statistics do not substantiate a surge of illegal immigrants through the Eastern Caribbean.

The Office of Border Patrol has one Station and Sector located in Ramey, Puerto Rico. This Sector and Station are located on the Western side of Puerto Rico and respond to their primary threat, which is illegal smuggling through the Mona Passage from the Dominican Republic. Ramey Sector has integrated its Intelligence Unit with other DHS partners to monitor traffic in its area of operation. The Ramey Border Patrol Sector enjoys a cooperative relationship with the U.S. Coast Guard and local Puerto Rican Maritime Police Forces (FURAS). The Coast Guard, Puerto Rican Police, CBP's Air and Marine Office all cooperate on interdictions and landings and share intelligence in a timely manner.

Question. Has there been an increase in the number of illegal alien interdictions or other evidence of an increased flow of illegal aliens to Puerto Rico or Florida from the Eastern Caribbean?

Answer. As noted above, CBP arrest statistics do not indicate that there is an increase in alien apprehensions from countries located in the Eastern Caribbean area or an increase in the flow of illegal aliens from the Eastern Caribbean to Puerto Rico and Florida.

Question. What is the status of discussions to open a Border Patrol Substation in the U.S. Virgin Islands?

Answer. CBP's priority mission is to prevent the entry of terrorists and terrorist weapons into the United States, and agency resources are allocated on the basis of risk assessment. The Northern Border represents a significant terrorist risk due to the presence of terrorist groups within Canada. In addition, aliens from special interest countries have been apprehended crossing the Southern Border using traditional alien smuggling routes. These indicators have to date not been manifested in the Caribbean. Therefore, although CBP continues to work closely with the U.S. Coast Guard to detect and interdict alien and drug smuggling activity in the Caribbean, CBP has not deployed additional resources in the area. CBP's Office of Intelligence is currently conducting a comprehensive risk analysis of the Caribbean, which will form the basis for making a future decision regarding the location of Border Patrol stations in the region.

COLLECTION OF ANTIDUMPING AND COUNTERVAILING DUTIES

Question. Senate Report 108–280 included specific language that directed Customs and Border Protection (CBP) to submit a report to the House and Senate Appropriations Committees by February 8, 2005. The report was to provide a coordinated plan, including legislative or regulatory changes proposed by CBP, if necessary, to increase CBP's collection of antidumping and countervailing duties owed to the United States. The Senate Appropriations Committee has not yet received that report. Will the report be delivered prior to the Subcommittee marking up the fiscal year 2006 bill in June?

Answer. The report was sent to the Committee on July 7, 2005.

Question. On December 17, 2004, Customs and Border Protection issued its regular Annual Report on the Combined Dumping and Subsidy Offset Act (CDSOA). The Annual Report described how hundreds of millions of dollars in duties are not being collected by Customs, and the agency has been unable to explain why it cannot collect these funds. In fiscal year 2003, the agency failed to collect $130 million in duties owed the United States under the U.S. antidumping and countervailing duty laws, and CBP failed to collect an additional $260 million in fiscal year 2004. The majority of that $390 million is the result of uncollected duties on goods imported from China.

What is CBP doing to solve this problem?

Answer. CBP disburse annually all antidumping duties available from entries that have been finally liquidated to domestic petitioners. The disbursements are made within 60 days of the end of the fiscal year.

CBP recognizes that imports of antidumping merchandise pose a financial risk to domestic industry. We share the concern regarding the lack of funds available for disbursement to domestic petitioners of antidumping duties. Therefore, CBP has instituted several aggressive actions to mitigate the collection risks going forward. We have a high degree of confidence that for entries received after the initiation of these new measures, the collection rate will improve.

—*Amendment to the Continuous Bond Guidelines.*—As of July 9, 2004, CBP has increased the continuous bond amount for importers of agriculture/aquaculture products subject to antidumping cases. The bonds will be set at a much higher rate, providing additional coverage in the event that an importer defaults. The new and proactive approach by CBP will provide the highest level of protection against default and directly addresses instances where the final liquidation rate is much higher than the initial deposit rate made at time of entry.

—*Integration With Other Agencies.*—CBP has recently begun working with the Department of Treasury to address the financial risks associated with sureties. Treasury conducts quarterly solvency evaluations of sureties and provides approval of the sureties to write customs bonds. By working together, we have developed a mechanism by which CBP can provide Treasury with data about sureties that are heavily weighted in "high-risk" transactions, such as antidumping. Treasury will incorporate this information in their solvency evaluation to mitigate the risk of surety bankruptcy. In addition, CBP is closely working with the Department of Commerce to find workable solutions to the challenges we face in collecting antidumping duty.

—*Increased Monitoring of Imports.*—CBP has taken measures to increase the monitoring of entries of agriculture/aquaculture products subject to antidumping duties. This monitoring provides a means to ensure compliance with bonding requirements, aids in the identity of surety risks, and helps thwart circumvention attempts. The closer scrutiny allows CBP to quickly identify new importers, particularly sham or shell companies. The monitoring provides CBP with the opportunity to raise bonds on these entities at once. By stepping up the monitoring of agriculture/aquaculture imports, CBP is also in a position to recognize shifts in patterns that may indicate circumvention attempts.

We believe that the new bonding methodology, working with other agencies, and closely monitoring imports will have a positive impact on the collections of antidumping duty, making more funds available for disbursement to the domestic industry.

CBP has taken a number of steps to ensure that the appropriate antidumping and/or countervailing duty (AD/CVD) revenue is collected. CBP has initiated centralization of all AD/CVD continuous bond activity for the bond program under the Revenue Division, Office of Finance, U.S. Customs and Border Protection in Indianapolis, Indiana. This establishes more uniform, consistent and effective management of continuous bonds involving AD/CVD. Also, AD/CVD bond formulas have been amended with an objective to minimize AD/CVD revenue losses as a result of bond insufficiency. The first commodity subject to this new bonding formula is shrimp.

Question. Why is this problem of non-collection growing, and what is CBP doing to address it?

Answer. Final liquidation for AD/CVD occurs several months, sometimes years after actual entry of the merchandise. The significant increase in uncollected antidumping duties seen in fiscal year 2003 reflected the first series of liquidation instructions for cases covering the types of merchandise we now understand to be problematic for collection; agriculture/aquaculture merchandise. These liquidation instructions covered entries going back as far as 1997 and 1998. The increase in uncollected antidumping duties in fiscal year 2004 reflects the growth in imports that was seen in years after the initiation of the cases, particularly the crawfish case. CBP is confident that collection rates will increase for entries received after the implementation of the measures highlighted in above.

CBP has taken several measures to maximize collection of AD/CVD revenue. Continuous bonds covering new AD/CVD merchandise are being managed as a part of the overall centralization of continuous bonds at the Revenue Division, Office of Finance, U.S. Customs and Border Protection in Indianapolis, Indiana. Also, AD/CVD bond formulas have been amended with an objective to minimize AD/CVD revenue losses from bond insufficiency. However, uncollected revenue will occur as a result of entry activity during years prior to affecting these new measures. As an example, although the Revenue Division has processed over 25,000 continuous bonds from the beginning of the centralization effort that began August 12, 2003, not one bond has

been subject to a collection action. Collection action is dependent on liquidation of the formal entry summaries covered by the bond. Liquidations may occur up to several years following the initial entry date. In addition, the amended AD/CVD bonding formula currently covers only shrimp.

Question. In past correspondence with my office, Commissioner Bonner indicated that CBP supported legislation that Senator Cochran and I introduced in the last Congress—and that we have reintroduced in the 109th Congress—to solve this problem of non-collection. That legislation, which passed the Senate unanimously last year, would require cash deposits instead of bonds in certain antidumping reviews. Would you be willing to express your support for this legislation directly to House Ways & Means Chairman Bill Thomas and other Members of the Congress, including the House leadership?

Answer. The Department and CBP are taking steps necessary to collect appropriate duties and provide appropriate funds to U.S. companies and workers through the Continued Dumping Subsidy Offset Act (CDSOA) disbursements. We agree that cash deposits in lieu of single-entry bonds may provide greater coverage and are less of an administrative burden. We are taking steps to provide greater security for the collection of AD/CVD within the framework of existing legislation, and are working with the Department of Commerce to apply more innovated methods to address these and other risks from imports subject to antidumping and countervailing orders. We look forward to continuing to work with Congress on ways to improve our performance in this area.

Question. As mentioned previously, in the past, U.S. industries like the U.S. crawfish industry have discovered only very late in the year that millions of dollars of antidumping duties for some reason have not been collected in their cases against Chinese imports as required by law. And, because CBP's failure to collect these duties has been discovered late in the year, the non-collection problem in these cases could not be addressed in time to enable the industries to obtain their yearly distribution of funds under the CDSOA. As a consequence, the U.S. crawfish industry, for example, last year failed to receive at least $54.4 million it otherwise would have received in duties paid the U.S. Government by Chinese importers. It is my understanding that CBP's Office of Information Technology (OIT) is fully capable of running an already existing program much earlier in each calendar year, (meaning by the end of March at the latest), which would enable both CBP and U.S. industries to learn, much earlier, if millions of dollars in duties are not being collected by CBP from U.S. importers of foreign, dumped products.

Why can't CBP's OIT determine by the end of this month if there are cases in which CBP is not collecting duties owed the U.S. Government and make that information publicly available as early as possible?

Answer. CBP has responded to the revenue risk posed by the inability to collect certain AD/CVD duties through several means, one of which is the monitoring the AD/CVD bills and collections on a more regular basis. For the distribution of these funds to take place timely, it is necessary not only to monitor the timely collection of AD/CVD duties but also to ensure our revenue collection system is protected from possible circumvention and corporate solvency schemes designed to enter AD/CVD goods into the U.S. market with the intention of never paying the proper duties at time of liquidation.

On a monthly basis, CBP is performing a risk-based review of outstanding bills for AD/CVD duties. The information has proven effective in identifying high-risk companies for AD/CVD evasion as well as improves the timeliness of our reviews. CBP is also focused on the long-term issue of the company's financial solvency and their ability to pay outstanding AD/CVD bills. The continuous bond guidelines for imports of certain agriculture/aquaculture imports were amended in July 2004 to address just such an issue. Working with the Department of Commerce, we are addressing the AD/CVD issues that pose the greatest risk.

Question. Again, two of the problems that CBP has exhibited with respect to its administration of the CDSOA are (1) CBP failure to collect duties rightfully owed; and (2) its failure to pay duties already collected in a timely fashion to eligible U.S. companies and their workers. With respect to the second problem, CBP sometimes holds, in what are called "clearing accounts," duties that are collected over many years—but for which the agency is awaiting final "liquidation instructions" from the Commerce Department prior to distribution. Often, the Commerce Department claims that such instructions have been sent, but CBP does not know they have been sent or never receives them. It has been proposed that one solution to this problem would be for CBP to publish the amount of funds held in CBP's clearing accounts, by administrative review period, so that CBP and Commerce can work together to determine which funds should have been liquidated and be available for distribution to eligible U.S. producers. CBP, in certain circumstances, has provided

such information to Members of Congress upon request, but has refused to provide such information generally.

Will you commit to identifying (i.e., publishing) the amount of funds held in clearing accounts by administrative review period?

Answer. The AD/CVD modules within the Automated Commercial System (ACS) do not provide information by administrative review periods; therefore, CBP cannot currently track entries in this manner. CBP has provided information of this type in certain circumstances through a manual review process. CBP is working towards including functionality in the Automated Commercial Environment (ACE) to identify and track AD/CVD data to ensure timely and accurate liquidation.

The OIG expressed concern about approximately one million entries suspended by CBP. As a result of this finding, CBP developed a plan to isolate those suspended entries that were beyond the normal timeframes of an AD/CVD case. Once identified, CBP worked with the Department of Commerce (DOC) to obtain liquidation instructions for these entries. To date, CBP has reduced the national inventory by 80,000 entries. CBP plans to continue to work with DOC to reduce the inventory substantially.

In fiscal year 2005, CBP is concentrating on the liquidation of remaining AD/CVD entries entered prior to 1995 that remain suspended. This action will remove approximately 50,000 entries representing over $46 million in deposits on 222 cases from the "official" inventory. By the middle of fiscal year 2006, CBP plans to liquidate the remaining 50,000 or so entries.

Another reason that monies remain in the "clearing accounts" and are unavailable for distribution via CDSOA is the number of protests on bills issued by CBP. Payment of a protested bill is deferred until the protest decision is rendered. Currently, many protests of AD/CVD liquidations are suspended pending the final decision by the Federal Appeal Court on International Trading.

Question. Will you commit similarly to identifying the reasons for the lack of liquidation in cases where liquidation has not occurred for more than 4 years, and provide specific information with respect to those cases showing the amounts that remain unliquidated accompanied by an explanation of CBP's understanding of why the amounts have not been liquidated?

Answer. Again, the AD/CVD modules within the ACS do not provide information by administrative review periods; therefore, CBP cannot track entries this way. This functionality will be programmed into the ACE and should be available by the end of fiscal year 2007.

STAFFING

Question. What was the CBP on-board strength (including AMO) on September 30, 2004? What was it on March 31, 2005? Provide the same data for the Border Patrol.

Answer. Air and Marine Operations employees were not transferred to CBP until October 31, 2004. The attached chart therefore provides on-board strength at two snapshots in time to reflect this transfer.

	October 2, 2004	April 2, 2005
Total CBP staffing		
CBP total	40,934	41,717
Border patrol agent staffing		
Border patrol Agents total [1]	10,817	10,859

[1] These amount are also included in the CBP totals above.

DETENTION FACILITIES

Question. One of the primary functions of the Bureau of Immigration and Customs Enforcement (ICE) is to serve as this country's interior line of defense by apprehending illegal entrants and detaining them pending the outcome of an administrative determination of their status. However I understand that ICE is considering closing the only secure, non-criminal detention center in New York City—the very site of the 2001 terrorist attacks—because of an apparent decision to focus the bulk of the agencies efforts on only identified criminal aliens and other high-risk illegal immigrants. This concerns me greatly because I understand that the vast majority of the individuals detained at this New York City detention facility would be released on their own recognizance into the New York City area.

Why is DHS proposing to close this detention facility in New York City? Is this because of a lack of funds? Are there not enough aliens needing to be detained which necessitates the closure of this facility?

Answer. In a continuing effort to consolidate detention capacity where possible in order to increase operational efficiency, ICE has decided not to exercise the next available option to extend contract performance at the Queens CDF.

The current contract was awarded to GEO on March 27, 2002. The Queens CDF provides detention housing and transportation of non-criminal detainees in the custody of ICE. A significant population designated to the Queens CDF is comprised of asylum seekers apprehended at POEs in the New York area.

The indefinite delivery/indefinite quantity contract includes a guaranteed minimum detainee population of 150 ($219.02 per manday) and a maximum capacity of 200 ($9.17 per manday exceeding 150 beds). The contract consists of a base year and 4-1 year options, exercised at the unilateral discretion of the government. The contract is currently performing within Option Year 2.

A recent assessment determined that a substantial number of the population routinely designated to the Queens CDF could be adequately managed through a combination of bonds, orders of own recognizance, and/or the increased use of alternatives to detention (e.g., electronic monitoring; telephonic reporting, etc.). All non-detention options will be applied based on established ICE standards. The remaining population requiring detention can be consolidated into substantially lower cost detention capacity available to ICE via commercial contracts and agreements with local government service providers. Other efficiencies will accrue from the consolidation of detainees, staff, the administrative hearing process, support programs, etc. These increased efficiencies will permit ICE to apply funds toward detaining higher priority cases.

It should also be noted that various non-governmental organizations have previously expressed concern regarding conditions of confinement at the Queens facility (See February 8, 2005 CIRF report, "Report on Asylum Seekers in Expedited Removal).

Utilizing all available options to manage the non-criminal alien population apprehended in the New York area and consolidating the population requiring detention into lower cost facilities, will result in improved efficiency in the ICE detention program.

Question. I understand that ICE makes an initial determination as to the level of risk of the illegal alien and that such a determination often is conducted at the point of entry which, in the case of this facility, is JFK International Airport.

How often does ICE make an initial determination that an individual is a "low-risk" illegal immigrant and then, after further investigation, determine that the individual should have been classified as "high-risk?"

Answer. The law enforcement databases used to track alien detention do not allow for us to determine the number of aliens who were initially considered "low risk" and are then later considered "high risk". These categories are used as guidelines in making the detention decision, but are not recorded as such in these databases.

Question. I believe these non-criminal detention facilities serve several purposes, one of the most important of which is holding those potentially high-risk individuals who fall through the cracks during the initial screening and who initially are misclassified as low-risk. Furthermore, I believe that facilities such as the one in New York City serve a very important deterrent effect. I understand that JFK Airport was a popular entry point for illegal immigrants prior to the opening of this New York City detention facility.

Does DHS believe that these types of facilities serve a deterrent effect and, more importantly, serve to catch high-risk individuals who might slip through the initial screening process?

Answer. Detention and removal are deterrents to illegal immigration. However, detention resources must be effectively managed to ensure that secure capacity is available to accommodate cases according to our detention priority continuum. It has been determined that a substantial number of the population routinely designated to the Queens CDF could be adequately managed through a combination of bonds, orders of own recognizance, and/or the increased use of alternatives to detention (e.g., electronic monitoring; telephonic reporting, etc.). All non-detention options will be applied based on established ICE standards. The remaining population requiring detention will be consolidated into substantially lower cost detention capacity available to ICE via commercial contracts and agreements with local government service providers. Other efficiencies will accrue from the consolidation of detainees, staff, the administrative hearing process, and support programs. These increased efficiencies will result in savings that can be applied to other immigration enforcement activities.

Question. Given the importance of these types of facilities, how can DHS justify their closure in New York City, especially when the only other facility in the general vicinity is designed to hold criminal aliens and which I understand operates at or near capacity?

Answer. A recent assessment determined that a substantial number of the population routinely designated to the Queens CDF can be adequately managed through a combination of bonds, orders of own recognizance, and/or the increased use of alternatives to detention (e.g., electronic monitoring; telephonic reporting, etc.). All non-detention options will be applied based on established ICE national standards. The remaining population requiring detention can be consolidated into substantially lower cost detention capacity available to ICE via commercial contracts and agreements with local government service providers. All cases requiring detention will be designated to appropriate conditions of confinement. Efficiencies will accrue from the consolidation of detainees, staff, the administrative hearing process, and support programs. ICE can use the savings from these increased efficiencies to detain higher priority cases.

MEASURES FOR DETERMINING BUDGETS

Question. What is the ratio or other measurement by which ICE determines how many detention beds are required in a given year? For instance, is there a ratio or determination made such that if one assumes that one Border Patrol agent is responsible for *x* apprehensions of illegal aliens then there is a need for *y* detention beds? And is there a similar ratio or measurement between the amount of bed space required because of the investigation success rate of ICE immigration investigators?

Answer. The Department is working aggressively to develop a comprehensive border control strategy that responds more effectively to alien apprehensions and the overall flow of illegal crossings. As fundamental improvements to the system are implemented through this strategy, we will implement systematic modeling that can more accurately link resources with apprehensions and other measures of demand.

WORKSITE ENFORCEMENT

Question. For Worksite Enforcement, how does ICE determine how it will focus its resources? For example, which areas or industries will be targeted?

Answer. Since September 11, 2001, ICE Worksite Enforcement activities have focused primarily on removing unauthorized workers from critical infrastructure facilities to reduce the risk of terrorist attack from insiders. ICE Critical Infrastructure Protection (CIP) operations are generally initiated at the local level and are based upon factors such as the type and number of infrastructure facilities present in each Special Agent-in-Charge jurisdiction (seaports, airports, military bases, defense contractors, nuclear plants, etc.) and upon specific or general threat information received from various intelligence sources, the general public, and from other law enforcement agencies.

ICE Worksite Enforcement activities also target criminal employers whose violations have a nexus to human smuggling, immigration document or benefit fraud, and worker exploitation. The authorities being enforced generally include one or more of the civil and/or criminal provisions of INA 274A (Unlawful Employment of Aliens). Many criminal employer investigations also result in the charging of violations relating to harboring, smuggling, and document fraud. The fiscal year 2006 Budget includes an increase of $18 million and an additional 140 agents to support the Temporary Worker Program.

CYBER CRIMES

Question. For fiscal year 2005, Congress provided $4.2 million for additional cyber crime forensic infrastructure and expansion of the Cyber Crime Center to ICE field offices. What is the status of this effort?

Answer. This funding provides for the creation of a wide area storage network for the ICE Computer Forensic Program. Upon award, disk storage arrays will be installed in four or five (final numbers are contingent upon final pricing) ICE field offices to provide storage for digital evidence under examination.

The ICE Cyber Crime Center has conducted a thorough market and technical analysis and is in the final stages of making a vendor selection.

An inter-agency agreement has been established with the U.S. Bureau of Public Debt (BPD) to utilize their existing IT procurement vehicle to make the contract award. The statement of work and performance work standard documents have been forwarded to BPD on August 18, 2005. It is anticipated that the contract will be awarded to TKC Communications of Fairfax, VA, an Alaskan native corporation,

shortly. Once awarded, site surveys, selection, and installations will begin in earnest.

Question. Have any of these funds been obligated?

Answer. None of the $4.2 million has been obligated.

Question. Have any additional personnel been hired?

Answer. No additional personnel will be hired with the $4.2 million.

Question. To which field offices, if any, will the Center expand?

Answer. This answer contains infomrmation considered Law Enforcement Sensitive and has been provided to the Committee under separate cover.

PASSENGER AIR FEES

Question. The Administration's budget for DHS proposes a significant increase to the security fee passengers pay by more than doubling the cost for the first leg of a flight from $2.50 to $5.50. These fee collections, if approved, would be used to pay for approximately 83 percent of the fiscal year 2006 budget request for the Transportation Security Administration. According to the Congressional Budget Office (CBO), this proposal would generate $1.680 billion in additional funding for fiscal year 2006.

Will a legislative proposal be sent to the authorizing committees with jurisdiction over this issue, and if so, when?

Answer. The fiscal year 2006 President's Budget provided a legislative proposal to modify this fee authority. In Title V—General Provisions, the proposal states, "SEC. 517. In Chapter 449 of title 49, United States Code, section 44940(c) is amended by striking '$2.50' and replacing it with '$5.50', and striking '$5.00' and replacing it with '$8.00'." This modification to the fee authority would allow TSA to implement the fee increases sought in the President's fiscal year 2006 Budget. TSA will work with the Appropriations Committees of the House and the Senate, as well as the appropriate authorizing committees in both bodies, to ensure enactment of the proposed security service fee increase.

Question. Second, if the proposed fee is not approved, will the Secretary urge the President to submit a budget amendment to fill the $1.7 billion funding gap?

Answer. The sharing of aviation screening costs between industry, passengers, and Government is essential to ensure that there is sufficient funding for existing and emerging threats to the integrity of the aviation security infrastructure. The proposed increase is intended to shift the burden of paying aviation screening services from the general taxpayer to the airline passenger. The Department will work with Congress to ensure that security priorities are met.

Question. Finally, what programs and activities does the Department propose be cut if the fee increase is not authorized by Congress?

Answer. The sharing of aviation screening costs between industry, passengers, and Government is essential to ensure that there is sufficient funding for existing and emerging threats to the integrity of the aviation security infrastructure. The proposed increase is intended to shift the burden of paying aviation screening services from the general taxpayer to the airline passenger. The Department will work with Congress to ensure that security priorities are met.

AIR CARGO

Question. Public Law 108–458, which was signed into law by the President on December 17, 2004, included an authorization for $100 million in fiscal year 2006 to accelerate the development of technologies to screen air cargo. The Administration's budget proposes that air cargo screening technology development be funded through the Science and Technology directorate, but funding is cut by $45 million from last year and funding is $70 million below the amount authorized in the Intelligence Reform Act. How is a cut of this magnitude justified? Has there been a break through in the development of detection technology for air cargo that justifies the proposed cut?

Answer. The fiscal year 2006 President's Budget transfers $109 million in R&D funds from TSA to the S&T Directorate. Of this amount, $29.578 million is dedicated to projects that will address air cargo screening capabilities. TSA retains $23 million in its fiscal year 2006 request to continue analyzing EDS products emerging from the Phoenix Phase II R&D program, piloting passenger screening projects, including next generation trace portal and automated checkpoint EDS, continuing EDS cargo break bulk evaluation, and conducting cargo technology field evaluations for field experiments.

The S&T Directorate does not plan to fund consolidated air cargo technology development outside those efforts captured by our broad R&D program, or captured in other efforts within the directorate, such as RFID technology, unless air cargo

pilots demonstrate the need and utility in specific cases, and focus instead on break-bulk inspection. Given a break-bulk inspection paradigm, the same technologies being explored for package or luggage inspection apply to cargo screening—and thus it is straightforward to include consideration of any specific requirements, e.g., size and throughput, into our broad R&D program.

With the fiscal year 2006 R&D funds, the S&T Directorate plans to conduct broad R&D that is applicable across the spectrum of baggage, package, and cargo screening. The S&T Directorate estimates that the funding required in fiscal year 2006 to complete the assessment of the efficacy of specific existing methodologies for particular cargo commodities, and to test screening procedures in the laboratory would be approximately $5 million. The Phoenix project is aimed at reducing false alarm probabilities in EDS systems, which is clearly beneficial to both baggage and package inspection. Other relevant RDT&E efforts within the aviation explosives detection efforts include nanotechnology-based sensors, CT array-based imaging (as opposed to rotating scans), and improved trace systems. Some of the TSA R&D projects funded in fiscal year 2005 will continue into fiscal year 2006 through completion of prototypes. These projects may continue to be funded by the S&T Directorate if they meet certain criteria, particularly in the area of break-bulk inspections.

Question. Public Law 108–458 authorizes $200 million per year for TSA to improve aviation security related to the transportation of cargo on both passenger aircraft and all-cargo aircraft. Why doesn't the fiscal year 2006 request include additional funding for air cargo security?

Answer. TSA's request for air cargo resources is at an appropriate level to ensure air cargo security and recognizes non-recurring system development costs while at the same time meeting all of the necessary transportation security priorities.

Question. Are there plans to increase the number of inspectors?

Answer. TSA currently employs 196 cargo inspectors. Three others have been selected and are in the final stages of the hiring process.

Question. Is TSA satisfied with 200 air cargo inspectors?

Answer. The President's fiscal year 2006 Budget request is a reflection of the resources required to ensure air cargo security and recognizes non-recurring system development costs while at the same time meeting all of the necessary transportation security priorities. Going forward, TSA will evaluate the needs and resources available to determine whether additional inspectors would be appropriate.

PRE-PACKAGED NEWS

Question. On March 16, the Washington Post printed an editorial entitled Viewer Beware. The editorial questioned the use of government-packaged and government funded news reports to look and sound like regular television reports. The editorial stated "Although this Administration apparently isn't the first to use video news releases, it seems more enamored of them than its predecessors. For example: A spot commissioned by the Transportation Security Administration lauds "another success" in the Bush Administration's drive to strengthen aviation security," which the reporter describes as "one of the most remarkable campaigns in aviation history." Unbeknownst to the viewer, the so called reporter was no reporter at all. She was a contractor hired by TSA. This type of pre-packaged reporting has occurred in other agencies as well, such as the Office of National Drug Control Policy (ONDCP) and the Department of Health and Human Services.

In every year since 1951, Congress has included a provision in the general government appropriations act which states the following: "No part of any appropriation contained in this or any other Act shall be used for publicity or propaganda purposes within the United States not heretofore authorized by Congress."

In recent cases involving prepackaged news stories by ONDCP and the Department of Health and Human Services, GAO concluded that those prepackaged news stories violated the publicity or propaganda prohibition. GAO did not receive a request to review the TSA story, but it was developed in a similar manner.

The Senate recently approved by a vote of 98–0 an amendment to the emergency supplemental to prohibit Federal funding of pre-packaged news stories unless the story includes a notification that it was created and funded by a Federal agency.

Do you agree that pre-packaged news segments produced by any DHS office should include a clear notification to the audience that the story was prepared or funded by that Federal agency?

Answer. DHS has a unique responsibility to provide Americans with important information they can use to be prepared for disasters, terrorist attacks or even to better navigate security procedures at our airports and ports-of-entry. Video news releases can serve as one tool for accomplishing this objective. We agree with the Ad-

ministration's previously articulated position that Federal agencies should be open about their activities and that DHS-produced Video News Releases (VNRs) should be clearly marked.

SCREENING WORKFORCE PERFORMANCE

Question. The DHS Inspector General recently released results of an audit on Transportation Security Administration screener performance.

The IG's audit indicated that the problems will most likely persist without greater use of new technology. The IG recommended that the TSA administrator aggressively pursue the development and deployment of innovations and improvements such as the backscatter x-ray and explosive trace detection portals to help the screener workforce better detect weapons and explosives. However, the Department's fiscal year 2006 budget actually reduces the amount of money included for Next-Generation explosive detection systems from $54 million to $49 million and significantly below the $100 million authorized in the Intelligence Reform Act.

In light if the sobering results of the IG audit, how can you justify reducing the amount of funding for the development and deployment of innovative detection technologies?

Answer. The TSA recognizes that additional resources must be devoted to address this critical vulnerability and improve the effectiveness of checkpoint screening. As it relates to deployment, TSA will have the ability to screen elevated risk passengers for explosives at all passenger checkpoints by January 2006. TSA will devote a total of $100 million to this initiative in fiscal years 2005 and 2006. In fiscal year 2005 TSA received $28.3 million to field emerging technology equipment at checkpoints. For fiscal year 2006, TSA is requesting a total of $72 million (an increase of $43.7 million over the fiscal year 2005 base amount) for emerging checkpoint explosives technology. In fiscal year 2005, TSA devoted $54 million for research and development (R&D) on Next Generation Explosives Detection Systems (EDS). The fiscal year 2006 Budget proposes to transfer TSA's R&D function to the S&T Directorate.

TSA SPENDING ABUSES

Question. The DHS Inspector General recently released a report that highlighted a laundry list of disturbing financial purchases relating to the creation of the Transportation Security Operations Center. For instance, $252,000 was spent on artwork, $30,000 was spent on expensive silk plants, money was used to buy leather brief cases and coffee pots, and over $83,000 in overpayments remains unaccounted for. There are even seven kitchens in the building for just 79 Federal employees located there. This report follows on the heels of the IG's findings last year that TSA provided excessive bonuses to its executives.

In response to these findings, A TSA spokesman said that "a new management structure" has been put in place "to strengthen its acquisition program to ensure responsible stewardship of taxpayer dollars." Please explain in detail what steps have been taken to change TSA's management structure to prevent such abuses from continuing.

Answer. Since its inception, TSA has worked to develop and implement a more responsive and robust acquisition program based on sound business management practices. The elevation of the Office of Acquisition within the agency is a key indicator of our commitment. Since the Transportation Security Operations Center (TSOC) lease process was initiated, the Office of Acquisition has been elevated to the Assistant Administrator level, equivalent to the Chief Financial Officer (CFO) rather than as a sub-program within the CFO's office. In late 2003, the Office of Acquisition stood up an Acquisition and Program Management Support division to focus on certifying, training, and providing day-to-day assistance to and for TSA's program managers. Well over 1,200 TSA employees have been trained to date in key acquisition topics and the Program Management certification program is robust.

At the beginning of fiscal year 2005, TSA took the following steps to help strengthen and mature its acquisition program in four key areas.

—Continue to support the TSA mission with efficient, expeditious, and accurate contracts. TSA recognizes that the agency's ability to attract, recruit, and retain qualified acquisition personnel to support contracts is critical to fulfilling its mission. Initial staffing in the Office of Acquisition was barely adequate to award contracts in time to meet Congressional deadlines, much less commence good business processes. Over the past year, TSA has raised the Office of Acquisition's staff ceiling by nearly 30 percent. Additionally, a percentage of TSA's budget has been earmarked for contract oversight, which includes support from

the Defense Contract Audit Agency and Defense Contract Management Command, and independent contractor support.

—Significantly improve acquisition and program planning. The Office of Acquisition is focused on strengthening the program planning function. The office developed and now coordinates an Investment Review Board process that drives successful program decisions by providing direct subject matter expert support to program managers. Additionally, the office provides direct support to program offices to assist them in developing sound acquisition and program strategies.

—Significantly improve program management and administration. Well-trained, certified program managers are fundamental to robust acquisition programs. These managers were, initially, in short supply at TSA. To address immediate knowledge gaps in key areas, the Office of Acquisition rolled out a set of workshops in October 2003. In early 2004, TSA worked with DHS to implement a Program Management certification program and the first TSA applications were received in June of 2004. Moreover, the Office of Acquisition developed a Management Directive regarding acquisition planning, review, and reporting that significantly tightens up the overall process.

—Build and mature the TSA acquisition infrastructure. TSA is focused on these two infrastructure areas: human resources and systems.

Human Resources.—In addition to increased staff, the Office of Acquisition is developing a longer-term strategic human capital plan to manage recruitment and retention issues, provide for career development, and succession planning. The plan will provide a roadmap for strengthening the current workforce (training, communication, professional development), as well as outline strategies to recruit highly qualified individuals and manage attrition. Simply put, the strategy will outline a plan to develop the right people with the right knowledge and skills for each of TSA's acquisition programs.

Systems.—On the systems level, TSA is implementing PRISM, an integrated finance and procurement system which will streamline and strengthen our processes and integrate acquisition with finance and asset management.

AIR CARRIER FEES

Question. The Government Accountability Office recently estimated that 2000 passenger and property screening costs incurred by air carriers was $448 million, $129 million less than what the air carriers paid to TSA. What plan of action will be taken by TSA as a result of GAO's estimates?

Answer. In the Homeland Security Appropriations Act, 2005, (Public Law 108–334) Congress directed the Government Accountability Office (GAO) to determine how much air carriers spent on security screening in 2000—the basis for the fee imposed on airlines. GAO completed its review and issued a report on April 18, 2005. The report concludes that the amount of the industry-wide passenger and property screening costs was between $425 million and $471 million, with a midpoint estimate of $448 million. The midpoint difference between what is collected now and what GAO indicates should be collected is $129 million. However, GAO's estimate did not include certain cost categories (e.g.; real estate, CAPPS, and positive bag match) due to the unavailability of information within the timeframe provided. The cost of these items could be significant. The TSA is currently reviewing all the findings of the report and developing a suitable overall implementation strategy for the air carrier fee.

SECTION 605 OF VISION 100

Question. The TSA budget proposes to defer use of allocation formulas required by Section 605 of Vision 100. Please provide a list, by airport, of all requests for assistance under the allocation formula program versus funding provided via Section 605. This list should distinguish between large hub airports, medium hub airports, and small hub airports.

Answer. TSA has received a number of requests from airports for funding to support construction of, or reimbursement for, in-line checked baggage screening solutions. Below is a list of the airports that have made these requests:

	Airports that have requested funding for an Inline System	Category	Notes
BWI	Baltimore-Washington International Airport	L	
DCA	Ronald Reagan Washington National Airport	L	
DTW	Detroit International Airport	L	
EWR	Newark International Airport	L	

	Airports that have requested funding for an Inline System	Category	Notes
FLL	Ft. Lauderdale-Hollywood International Airport	L	
HNL	Honolulu International Airport	L	
IAD	Washington-Dulles International Airport	L	
IAH	George Bush Houston Intercontinental Airport	L	
JFK	John F. Kennedy International Airport	L	
LGA	LaGuardia Airport	L	
MCO	Orlando International Airport	L	
MDW	Chicago Midway International Airport	L	
MIA	Miami International Airport	L	
MSP	Minneapolis-St. Paul International Airport	L	
OAK	Metropolitan Oakland International Airport	L	
ORD	Chicago O'Hare International Airport	L	
PHL	Philadelphia International Airport	L	
SAN	San Diego International Airport	L	
SFO	San Francisco International Airport (reimbursement)	L	
SLC	Salt Lake City International Airport	L	
TPA	Tampa International Airport	L	Current in-line system
ANC	Anchorage International Airport	M	
BDL	Bradley International Airport	M	
BNA	Nashville International Airport	M	
CLE	Cleveland-Hopkins International Airport	M	
MCI	Kansas City International Airport	M	
MKE	General Mitchell Milwaukee International Airport	M	
OGG	Kahului Airport Maui	M	
PDX	Portland International Airport	M	
PVD	Providence T F Green State Airport	M	
RSW	Southwest Florida Fort Myers International Airport	M	
SAT	San Antonio International Airport	M	
SJC	San Jose International Airport	M	
SMF	Sacramento International Airport	M	
SNA	Orange County John Wayne Airport	M	Current in-line system
BIS	Bismark Municipal Airport	N	
LNK	Lincoln Municipal Airport	N	
ACY	Atlantic City International Airport	S	
GEG	Spokane International Airport	S	
GPT	Gulfport-Biloxi International Airport	S	
MDT	Harrisburg International Airport	S	Current in-line system
PSP	Palm Springs International Airport	S	
TLH	Tallahassee Regional Airport	S	
VPS	Okaloosa Regional Airport	S	

Category: small (s), medium (m), large (l) or non-hub (n).

BASE DECREASES

Question. On page 38 of the TSA budget request, there is a reduction of $15.9 million for "management and technology efficiencies" and a reduction of $53.9 million for a "base realignment adjustment." There is no additional justification or information relating to those reductions. Provide a detailed justification for those decreases including a list of all management and technology efficiencies and how realigning the base saves $53.9 million.

Answer. The attached spreadsheet provides a detailed explanation of program reductions and base adjustments that resulted in $53.9 million in savings.

	FY2005 Proposed Spendplan	FY 2005 Enacted	Annualization of FY 05 Pay	Efficiency[1]	PAY/ NON PAY	Xfer Out	Remix & Program Decreases	Total FY 06 Base	Passback/Final Appeals Apprvd	Total	Comments
I. Aviation Security											
A. Screening Operations											
1 Screener Workforce	**2,557,001**	**2,424,000**						**2,489,003**		**2,668,984**	
Privatized Screening	152,654	129,654		(436)	1,985			131,151	15,000	146,151	Funding to support continued PP5 operations & increase workman comp. Bill.
Screener-PC&B	2,404,347	2,294,346	11,174	(8,943)	61,275			2,357,852	164,981	2,522,833	Funding required to support 45K screener FTE reflects a base adjustment.
2 Screener Training and Other	**438,574**	**494,274**						**468,484**		**468,484**	
Screener Consumable Supplies & Other	122,217	187,071		(751)	3,051		(31,328)	158,043		158,043	In order to stay within FY06 budgetary constraints, TSA scaled back field operations travel/consumables, uniforms, tort claims and preventative maintenance purchases to provide an offset for screener pay and benefits, human resources (HR) services, and in
Screener Training	94,364	145,000		(544)	2,220		(55,672)	91,004		91,004	Increasing the number of training classes conducted by TSA Approved Instructors and decreasing contractor instructed training.
Representation Funds	3	3						3		3	
HR Services	210,200	150,000		(563)	2,297		55,500	207,234		207,234	Funding required to support 45K screener FTE reflects a base adjustment.
Model Workplace	2,200	2,200					200	2,400		2,400	
Hazardous Material Disposal	9,600	10,000					(200)	9,800		9,800	
3 Checkpoint Support	**125,109**	**123,500**						**113,761**		**157,461**	
Checkpoint Reconfiguration	13,200	13,200		(75)	245		(3,370)	10,000		10,000	
Magnetometers	1,609										
Checkpoint equipment	37,000	37,000		(113)	459		(7,000)	30,346		30,346	In order to stay within FY06 budgetary constraints, TSA reduced the rate of purchasing new checkpoint equipment, emerging technology, and electronic surveillance equipment for airports to ensure adequate funding for existing equipment, and to provide an o
Electronic Surveillance	14,000	14,000		(38)	153		(4,000)	10,115		10,115	
Maintenance for Chkpt Equip.	31,000	31,000		(113)	460		3,653	35,000		35,000	The Sept. 11th Commission recommended that TSA take immediate action to improve explosives screening of all higher risk passengers at airport screening checkpoints. TSA will invest $100M between FY05 & FY06 for emerging checkpoint explosives technology.
Emerging Technology	28,300	28,300						28,300	43,700	72,000	
4 Secure Flight	**34,922**	**34,919**				(34,919)					
5 Crew Vetting	**10,038**	**10,000**				(10,000)					
6 Registered Traveler Program	**15,099**	**15,000**				(15,000)					Transfer to SCO
7 EDS/ETD Systems	**609,839**	**399,940**						**367,000**		**367,000**	
EDS/ETD Purchase	180,104	180,000		(563)	2,297		(51,734)	130,000		130,000	FY06 adjustments based on: maintaining LOI reimbursement levels at 75% and 90% for large and smaller airports, respectively, and the elimination of Aviation Security Capital Fund formula distribution requirements; fewer purchases of equipment required f

	FY2005 Proposed Spendplan	FY 2005 Enacted	Annualization of FY 05 Pay	Efficiency[1]	PAY/ NON PAY	Xfer Out	Remix & Program Decreases	Total FY 06 Base	Passback/Final Appeals Apprvd	Total	Comments
EDS/ETD Install	249,534	45,000					(31,000)	14,000		14,000	
EDS/ETD Maintenance/Utilities	186,201	174,940		(657)	2,679		23,038	200,000		200,000	
Operational Intergration						23,000		23,000		23,000	
Sub-Total Screening Operations	3,790,582	3,501,633	11,174	(12,848)	77,121	(36,919)	(101,913)	3,438,248	223,681	3,561,929	
B Aviation Direction & Enforcement											
1 **Aviation regulation & other**	225,601	230,000						232,196		238,196	
K-9 Units	20,000	20,000	83	(56)	260		(1,200)	19,087		19,087	In order to balance competing requirements within the budget, TSA will maintain K-9 efforts slightly below FY05 level to provide an offset for screener pay and benefits, human resources (HR) services, and information technology.
State and local	70,000	70,000		(263)	1,072			70,809		70,809	
Airport regulation & inspections	135,601	140,000	682	(525)	2,143			142,300	6,000	148,300	Increase funding by $6M and 31 FTE for foreign and domestic repair station inspection operations to meet the requirements of Vision 100 - Century of Aviation Reauthorization Act - and ensure that Foreign and Domestic Repair Stations are inspected.
2 **Airport mgmt, IT & Support**	566,382	526,890	1,383	(1,069)	4,348		(9,000)	584,370		758,370	
Airport Management and Staff	270,000	284,000		(375)	1,531			279,662		279,662	
Airport Rent and Furniture	100,000	100,000		(56)	243			101,156		101,156	
Airport Parking & Transit Benefits	15,890	15,890						16,077		16,077	
Airport Staff Info Tech	143,300	85,000		(413)	1,684		81,070	167,341		167,341	This increase of 81.07M is an adjustment to accurately reflect IT's base and align it with the assumptions in the FY 2005 reprogramming request.
Hi Soc Initiative									174,000	174,000	$174M completes the installation of HI-SOC connectivity TSA-wide.
Sabre	20,192	25,000		(94)	383		(22,369)	2,930		2,930	Sabre development complete. Reduction represents investment costs no longer required to create the screener scheduling information system. TSA will retain operating funds to maintain system in FY06 and the outyears.
Transportation Security Coordination Center	17,000	17,000		(56)	260			17,204		17,204	
3 **Flight Crew Training**	27,000	25,000						25,289		35,289	
Federal Flight Deck Officers	25,000	25,000		(94)	383			25,289	7,000	32,289	The $7M increase is required to recertify and requalify the current FFDO population while continuing to meet the demand for addition FFDOs.
Crew Member Self Defense	2,000								4,000	4,000	To provide for the first full year of the voluntary self-defense training program for flight and cabin crewmembers.
4 **Air Cargo**	43,365	40,000	146	(113)	459		(492)	40,000		40,000	
Sub- total Aviation Direction & Enforcement	862,348	821,890	2,294	(3,114)	12,766		48,019	881,855	191,000	1,072,855	
Subtotal - Aviation Security	4,652,930	4,323,523	13,468	(15,962)	89,887	(36,919)	(53,894)	4,320,103	414,681	4,734,784	

EMERGING CHECKPOINT EXPLOSIVES TECHNOLOGY

Question. For fiscal years 2005 and 2006, provide a deployment schedule, including the identification and cost of the technology acquired, the manufacturer of the technology, and the airports at which the technology has been or will be deployed.

Answer. The following list of airports (Fig. 1) will have checkpoint Explosives Detection Trace Portals deployed by January 2006. TSA is deploying the systems concurrently, therefore the list does not reflect any sort of priority. The timing for deployment between now through January 2006 will depend on the results of site surveys that are currently underway and the production capabilities of the vendor.

TSA will be purchasing two different portals, the GE Ion Track Entry Scan and the Smiths Sentinel, and the results of the site surveys will help TSA determine which of the two technologies is best suited for each of the airports listed. TSA is planning to purchase equal numbers of each of the two products.

In fiscal year 2005, TSA received $28.3 million to field emerging technology equipment at checkpoints. For fiscal year 2006, TSA is requesting a total of $72 million (an increase of $43.7 million over the fiscal year 2005 base amount) for emerging checkpoint explosives technology.

In support of checked baggage screening, the following list of airports (Fig. 2) will have the Reveal Technologies CT–80 deployed by January 2006. Like the checkpoint Explosives Trace Detection Portal, TSA's intent is to deploy the CT–80s concurrently, therefore this list does not reflect any sort of priority. The timing for deployment between now through January 2006 will depend on the results of site surveys that are currently underway and the production capabilities of the vendor. Consistent with the direction provided in the Homeland Security Appropriations Act, 2005, $30 million will be spent for purchase and installation of this capability.

FIG.1—EXPLOSIVES DETECTION TRACE PORTALS

	Airport
ATL	Hartsfield-Jackson Atlanta International
BOS	Boston Logan International
BWI	Baltimore/Washington International
CLE	Cleveland-Hopkins International
CLT	Charlotte/Douglas International
CMH	Port Columbus International
CVG	Cincinnati/Northern Kentucky International
DCA	Ronald Reagan Washington National
DEN	Denver International
DFW	Dallas/Ft. Worth International
DTW	Detroit Metropolitan Wayne County
EWR	Newark Liberty International
FLL	Fort Lauderdale/Hollywood International
HNL	Honolulu International
IAD	Washington Dulles International
IAH	Houston Intercontinental
IND	Indianapolis International
JFK	John F. Kennedy International
LAS	McCarran International
LAX	Los Angeles International
LGA	LaGuardia International
MCI	Kansas City International
MCO	Orlando International
MDW	Chicago Midway International
MIA	Miami International
MSP	Minneapolis-St. Paul International
OAK	Metropolitan Oakland International
ORD	Chicago O'Hare International
PBI	Palm Beach International
PDX	Portland International
PHL	Philadelphia International
PHX	Phoenix/Sky Harbor International
PIT	Pittsburgh International
RDU	Raleigh-Durham International
SEA	Seattle-Tacoma International
SFO	San Francisco International
SJU	Luis Munoz Marin International

FIG.1—EXPLOSIVES DETECTION TRACE PORTALS—Continued

	Airport
SMF	Sacramento International
SNA	John Wayne Airport-Orange County
STL	Lambert-St. Louis International
TPA	Tampa International

FIGURE 2.—REVEAL TECHNOLOGIES CT–80

	Airport
ABE	Lehigh Valley International
ACY	Atlantic City International
ALB	Albany International
BGR	Bangor International
BIL	Billings Logan International
BTV	Burlington International
CHS	Charleston AFB/International
ELP	El Paso International
EYW	Key West International
FAI	Fairbanks International
GPT	Gulfport-Biloxi International
GSP	Greenville-Spartanburg International
HGR	Hagerstown Regional-Richard A Henson Field
HPN	Westchester County
HSV	Huntsville International-Carl T Jones Field
ISP	Long Island MacArthur
LGB	Long Beach/Daugherty Field
MRY	Monterey Peninsula
OMA	Eppley Airfield
ORF	Norfolk International
PIE	St. Petersburg-Clearwater International
RNO	Reno/Tahoe International
ROC	Greater Rochester International
SWF	Stewart International
SYR	Syracuse Hancock International
TYS	McGhee Tyson

Question. Has the checkpoint technology that has been deployed been verified by the Science & Technology Directorate?

Answer. TSA works closely with the S&T Directorate and discusses its ongoing R&D efforts to ensure the S&T Directorate is not only aware of but supports TSA's efforts related to technology development.

HAZARDOUS MATERIALS ENDORSEMENT FOR COMMERICAL DRIVER'S LICENSE

Question. On January 13, 2005 a final rule was published in the Federal Register which established a fee for individuals who apply for or renew a hazardous materials endorsement for a commercial driver's license. According to the final rule, TSA intends to use fees collected under this rule to pay for the costs of the security threat assessments and the costs of collection and transmission of finger prints and biographical information.

Please provide the committee with an estimate of the amount of money these new fees are expected to bring in.

Answer. By law, the fees for individuals who apply for or renew a hazardous materials endorsement for a commercial driver's license cannot be collected in excess of the expenses to run the program. Accordingly, the program is expected to cost about $9 million in fiscal year 2005 and approximately $28 million in fiscal year 2006. The original fiscal year 2006 estimate of $44 million was adjusted mainly due to the change in the estimated HAZMAT applicant population.

PRIVATE SCREENERS

Question. The budget proposes an increase of $15 million to continue the privatized screening contracts at the current service levels. Explain why an additional $15 million is necessary when, currently, only one airport has applied for a

private screening workforce. Does TSA still anticipate the current number of airports participating in privatized screening contracts to remain the same?

Answer. As of May 2005, the Screening Partnership Program (SPP) had received a total of seven applications, which includes the original contract screening pilot program (PP5) airports (San Francisco, Kansas City, Rochester, Jackson Hole and Tupelo), and two new airports (Elko, Nevada and Sioux Falls, South Dakota).

In directing TSA to establish PP5, ATSA required that the level of screening services and protection provided at the PP5 airports be equal to or greater than the level provided at an airport with Federal screeners. Similarly, contract screeners must receive compensation and other benefits that are not less than the compensation and other benefits provided to Federal personnel. In accordance with these requirements, TSA strives for a level playing field between airports with private contract screeners under PP5 and the SPP and airports with Federal screeners. Consequently, as each airport considers whether to continue with Federal screening or to apply for the SPP, it can base its decision on its own preferences and criteria rather than considerations of security, resources, or level or service.

The additional $15 million requested is reflective of the increased cost of providing screening services at the levels required under ATSA. TSA is not funding services in addition to those provided in previous years except where consistent with changes in the Standard Operating Procedure made effective throughout the Nation's commercial aviation system.

In fiscal year 2005, a reprogramming increase of $23 million was made to support the cost of providing PP5 airports with the level of screening required for all commercial airports under ATSA. This reprogramming supported increased insurance premium costs for worker's compensation, terrorism and health insurance premiums, ATSA-guaranteed screener pay parity, and operational requirements relating to flexibilities granted to contractors in the areas of recruitment, hiring, and training.

Question. Are any of the airports currently participating planning or considering opting out of the private screening program?

Answer. TSA has received applications from all five private screening pilot airports to participate in the SPP.

Question. Are other airports not currently participating in the program planning to opt in?

Answer. While several airports have expressed interest to TSA about participating in the SPP, to date, only Elko Regional Airport and Sioux Falls Regional Airport have formally applied.

FOREIGN AND DOMESTIC REPAIR STATION INSPECTIONS

Question. The budget request includes $6 million for Foreign and Domestic Repair Station Inspection Operations. Does TSA have a schedule to inspect the 664 Foreign and Domestic Repair Stations? If so, provide the schedule to the Committee.

Answer. TSA has developed a Notice of Proposed Rulemaking (NPRM) that will increase security at both foreign and domestic repair stations. The NPRM is currently under Departmental review and is expected to be released for public comment in late summer of 2005. The agency has not yet developed a firm schedule for auditing all foreign repair stations. TSA is currently developing a survey document that will be sent to repair stations to assess their operations. This effort will assist in determining which repair stations pose the greatest potential risk and should be given priority for audits. TSA is also developing the necessary assessment tools for use by the inspectors during their visits to repair stations.

TSA fully expects to have developed the assessment tools necessary for the auditing effort by the time the final rule for repair station security is released, which TSA expects to occur by spring 2006. The actual schedule of audits will be dependent upon the initial survey of repair stations, which will begin as soon as the final rule is released.

Question. Is $6 million and 31 FTE the full amount necessary to inspect all Foreign and Domestic Repair Stations and the domestic maintenance, repair and overhaul facilities in the United States? If not, how much is needed to comply with "Vision 100?"

Answer. TSA would like to note that the $6 million and 31 FTE are earmarked solely for audits of foreign repair stations, of which there are approximately 650. There are approximately 4,500 repair stations in the United States, and current plans are to cover domestic audits with the existing force of Aviation Security Inspectors (ASI). Approximately 950 ASIs are presently assigned to geographical areas across the United States and inspect all facets of regulated aviation assets, not just repair stations.

The hiring projection with the $6 million requested in the fiscal year 2006 Budget is 12 inspectors, one program manager, and one program analyst. It is anticipated that additional foreign repair station inspectors, plus a manager and analyst, will be hired over a three-year time period. The hiring and operating projection costs of the program for its second and third years will be more accurately approximated after TSA assesses the costs of the initial year of the program.

TSA R&D

Question. The budget proposes to consolidate TSA R&D activities within the Science and Technology (S&T) Directorate. However, only $109 million is proposed for fiscal year 2006 within the S&T budget. TSA's budget maintains $23 million for operation R&D activities, such as pilot projects. Please explain why the program is proposed to be cut by $46 million and what impact that would have on ongoing R&D activities and those planned prior to the transfer proposal.

Answer. The $46 million consists of the following reductions: $25 million from Air Cargo R&D and $21 million from Explosives Detection Equipment (EDS) R&D. The reductions are appropriate given maturing technology in both areas, which, for example, will result in the deployment of Explosive Detection Trace Portals to 41 airports by the end of January 2006.

Overall, the reductions will have minimal effect on the R&D activities that would have been undertaken by TSA because those activities were budgeted by TSA and included in the proposed amount of $109 million.

REGISTERED TRAVELER

Question. Last year, TSA indicated that, assuming there was sufficient national interest in the program, the $15 million provided in fiscal year 2005 would be used for start-up operational costs and future funding would be generated by fees incurred by participants. What is the amount anticipated in fiscal year 2006 from offsetting collections?

Answer. TSA envisions a fully operational RT Pilot Program to be fee funded. The President's fiscal year 2006 Budget proposal includes $22.5 million from potential offsetting collections for RT, which was consolidated into the proposed SCO. However, TSA will need to implement a fee rule to accept fees for RT.

Question. What is the timeline and deployment schedule for implementing this program beyond the pilot stage?

Answer. Through a series of concurrent stand-alone pilots, TSA has been aggressively testing the RT concept of running threat assessment and identity verification checks on eligible volunteers in order to provide them with an expedited clearance through security checkpoints. TSA is currently running successful programs at five Federally managed pilot sites (Minneapolis, Los Angeles, Houston, Boston, and Washington, D.C.), which are scheduled to be completed in September 2005. TSA is concurrently working with the GOAA to launch a sub-pilot at Orlando International Airport in summer 2005 that will assess the feasibility of incorporating a private sector component into the RT concept.

Results of these pilots will be analyzed to determine the program's effect on security and service, enabling the Department to make decisions about full scale implementation of RT. Any timeline and deployment schedule for implementing RT beyond the pilot stage will be linked to the Department's decision.

DEEPWATER BUDGET

Question. Virtually the entire increase requested for Deepwater in fiscal year 2006 is just to sustain legacy assets. The revised Deepwater plan indicates that the lifecycle costs to sustain legacy assets could cost anywhere between $828 million and $1.8 billion. Why is there such a large difference between these two amounts?

Answer. The difference the two amounts is a function of time and money. The lower number reflects a lower total acquisition cost ($19 billion) over a shorter implementation period (20 years). The higher legacy asset funding amount reflects a higher total acquisition cost ($24 billion) over a longer implementation period (25 years). The shorter plan invests less funding in legacy sustainment, decommissions legacy assets sooner, but commissions fewer new assets. The longer plan invests more in legacy sustainment to keep the assets in commission longer, invests more in technology refresh/obsolescence prevention (i.e. life cycle costs), and delivers more new assets. Earlier decommissioning of legacy assets translates into lower legacy sustainment costs, but equates to a lower number of assets to perform Coast Guard missions both during build out and upon completion.

Question. What is the Coast Guard doing to better plan and prepare for legacy asset sustainment?

Answer. The Coast Guard has a detailed plan for maintaining its legacy cutters and aircraft. Coast Guard men and women are well trained to maintain and continually upgrade Coast Guard aviation, surface, and shore infrastructure assets. A mature project planning and execution program exists within the Coast Guard to provide routine unit-level and depot-level maintenance. Where expertise or infrastructure doesn't exist organically within the service, the Coast Guard uses contracted resources to provide the requisite maintenance support. Maintaining a high proficiency level amongst the Coast Guard's "maintainers" is critical to the long-term health of the service. One of the service's guiding principles is to maintain a core competency of maintenance expertise amongst Coast Guard (military and civilian) members to ensure service readiness, especially during periods of national emergency.

The Coast Guard maintains its legacy aircraft and vessels using organic maintenance and repair infrastructure in conjunction with contracted depot-level maintenance activities. These operating expense (OE) funded maintenance efforts are complemented by periodic Acquisition, Construction and Improvement (AC&I) projects which either enhance/sustain asset capabilities and extend asset service lives, or replace assets.

On April 20, 2005, the Coast Guard submitted a legacy asset report to Congress, detailing the Coast Guard's legacy asset issues. This report reflects legacy cutter and aviation AC&I projects that the Coast Guard has included in the fiscal year 2006 Budget request and anticipates requesting in future budget submissions.

Question. The Coast Guard's capital investment plan indicates that the Deepwater budget will be decreased by $214 million in fiscal year 2007. How can you propose such a cut in light of increasing mission demands and the "declining readiness" of existing assets?

Answer. The President's fiscal year 2006 Budget requests $966 million for Deepwater, $242 million above the fiscal year 2005 enacted levels, to fund critical modernization initiatives such as production of the third National Security Cutter and design and long lead material purchase for the Offshore Patrol Cutter while addressing immediate legacy asset issues such as HH–65 re-engining and Medium Endurance Cutter mission effectiveness programs. The Coast Guard's fiscal year 2006–2010 Capital Investment Plan contains $752 million for Deepwater in 2007 to highlight the one-time nature of several of these investments in legacy asset conversions and sustainment projects.

Question. The GAO recently testified that the Coast Guard has acknowledged that it needs to develop condition measures that more clearly demonstrate the extent to which asset conditions affect mission capabilities, but such measures have not been finalized or implemented. What is the Coast Guard's schedule for putting such measures in place?

Answer. To track the condition of the its cutters, the Coast Guard currently measures a Percent of Time Free (POTF) of major casualties measure that shows the general decline in condition of Deepwater legacy assets between 2000 and 2004. To track the condition of the its aircraft, the Coast Guard currently measures aircraft availability rates. However, as GAO has pointed out, "the Coast Guard's available condition measures are inadequate to capture the full extent of the decline in the condition of deepwater assets with any degree of precision." and Justice Issues, testified to the House Committee on Transportation and Infrastructure that, "Other evidence we gathered, such as information from discussions with maintenance personnel, point to conditions that may be more severe than the available measures indicate."

The Coast Guard acknowledges that it needs better condition measures to more accurately depict the condition of its assets. To address this issue, the Coast Guard is developing condition measures that more clearly link cutter condition to mission capability. This effort is scheduled for completion by the end of fiscal year 2005.

In fiscal year 2004, a team of personnel was assembled from engineering support activities in both Atlantic and Pacific Areas to work with Coast Guard Headquarters to construct an asset condition matrix that incorporates engineering casualty reporting (CASREP) data and performance data maintained in the Coast Guard's Readiness Management System (RMS). To do so, the team is identifying/linking thousands of shipboard engineering subsystems across every cutter class and their direct impact/contribution to each Coast Guard mission.

By establishing a clear relationship between engineering subsystems and mission performance, the Coast Guard will be better able to identify return on its maintenance investments and determine the best use of limited maintenance resources.

The Coast Guard is currently working to develop a comparable measure for its aviation assets; however, it has not established a timeline for implementation.

Question. The GAO report also noted that certain legacy costs, such as maintaining the 378-foot class through 2016 instead of 2013 as originally planned, is not addressed in the revised Deepwater budget baseline. How much funding will this require and are there other legacy assets that need further maintenance but are not included in the revised Deepwater plan?

Answer. Legacy asset sustainment is a Coast Guard stewardship priority that requires judicious balancing of current and future demands on limited AC&I investment resources. One of the primary determining factors is how long the asset class will remain in service. The 378-foot High Endurance Cutters (WHEC) are the first legacy cutters expected to be removed from service as the National Security Cutters (NSCs) are deployed. Therefore, the Department and the Coast Guard have invested AC&I funds toward acquisition of NSCs vice sustaining WHECs. Until they are decommissioned, WHECs will be sustained through routine depot level maintenance funded within the Coast Guard's Operating Expense Appropriation. The 210-foot and 270-foot medium endurance cutters are projected to remain in service longer, therefore substantial AC&I investments are being made in these classes in the form of Mission Effectiveness Program funds sought in fiscal year 2006 and in the outyears. Similar legacy sustaining initiatives are funded in the Deepwater implementation plan for aircraft that will remain in the Coast Guard's final Deepwater inventory. Additional details on the Coast Guard's plan to sustain its legacy assets are provided in a report that was submitted to Congress on April 20, 2005.

Question. What measures have the Coast Guard put in place to ensure that competition is built into Deepwater acquisition decisions?

Answer. From the beginning of the acquisition process, the Coast Guard has ensured competition has been built into the Deepwater program. The GAO recently reported that all assets originally planned for the first five years of the contract were properly competed through the initial contract award process that resulted in selection of Integrated Coast Guard Systems (ICGS) as the Deepwater contractor. Beyond the initial contract award process, the Coast Guard has taken several steps, including implementing GAO recommendations to ensure acquisitions decisions are adequately competed. There are many examples of competition in subcontracts that can be provided, if desired. For example, where changes to the original proposal have been introduced into the acquisition, the Coast Guard ensures that a competitive price determination is made. The price of this change order must be determined to be fair and reasonable before the Coast Guard will approve ICGS action. The Coast Guard monitors ICGS' use of the open business model as required by their internal procedures for second-tier subcontractors. ICGS also requires the first-tier subcontractors to encourage 2nd and 3rd tier suppliers to promote competition.

Question. What is the cost comparison of re-engining the existing fleet of HH–65 aircraft versus the procurement of a new aircraft outfitted to perform the same mission?

Answer. Re-enginging an HH–65 helicopter costs approximately $3 million. It would cost approximately $19 million to buy a new, commercial aircraft capable of performing the missions of a re-engined HH–65. Under the revised Deepwater implementation plan, HH–65 helicopters will receive additional upgrades to become multi-mission, cutter helicopters. The total cost of the re-engining and the upgrade to Multi-Mission Cutter Helicopter (MCH) is slightly less than $7 million per unit. To replace the entire HH–65 fleet would cost $1.8 billion vice $636 million for upgraded HH–65s, three times as much. It should also be noted that when the Coast Guard made the decision to re-engine the HH–65s it was in the face of a crisis in engine safety and reliability. Timely resolution of that crisis did not allow for acquisition of a replacement fleet. Further, HH–65 re-engining was already planned as part of the Deepwater solution. Re-engining was the most timely, cost-effective short and long-term solution.

Question. What is the status of the HH–65 re-engining process?

Answer. In August 2004, the first re-engined HH–65 was delivered to the Coast Guard at Aviation Training Center Mobile, AL, for operational testing and evaluation. As of the first of September 2005, 10 re-engined HH–65Cs had been delivered for full operational status to Air Station Atlantic City, NJ, (5), Aviation Training Center Mobile, AL, (1), and Air Station Savannah, GA, (4). To accelerate the HH–65 re-engining project the Coast Guard and its contractor, Integrated Coast Guard Systems (ICGS), have examined the quality and suitability of a second re-engining facility located in Columbus, MS. In August 2005, this facility delivered its first re-engined aircraft to the Coast Guard. This aircraft was determined to meet needed quality and suitability parameters and the Coast Guard contracted with ICGS to re-engine an additional 11 aircraft at the Columbus facility. The Coast Guard plans to have all 84 operational aircraft re-engined in early 2007.

Question. Will the 24 month schedule be met?

Answer. Provided the President's fiscal year 2006 request of $133.1 million for HH–65 re-engining is fully funded, the Coast Guard's plan is to complete re-engining the operational fleet of 84 helicopters by February 2007. This is the fastest possible production schedule based on the availability of engine kits and parts, maximum production at Coast Guard Aviation Repair and Supply Center, additional production capacity that may become available at a second facility, and number of aircraft that can be removed from operational service at any given time.

Question. What is the current timetable?

Answer. The first re-engined HH–65 was delivered for operational test and evaluation in August 2004. Regular production delivery of operational HH–65 began in April 2005, when the second HH–65 was returned to operational status at Air Station Atlantic City, NJ. Four others are scheduled for delivery in May 2005. In fiscal year 2005, a total of 29 conversion starts are planned. In fiscal year 2006, 51 conversion starts are planned. All 84 operational aircraft are scheduled for completion early in fiscal year 2007. Re-engining of all 95 HH–65s is scheduled to be completed in 2007.

Question. What barriers exist that could the Coast Guard from meeting this schedule?

Answer. The current timetable, resulting in completing the re-engining of the Coast Guard's operational fleet of 84 HH–65 helicopters, is based on the best outcome of a number of variables. To achieve this schedule there must be:

—Full support of the President's Budget request for $133.1 million in fiscal year 2006 funding for re-engining;
—Maximum availability of engine kits and parts;
—Effective mitigation of operational needs to maximize the number of aircraft that can be removed from operational service at any given time;
—The highest possible production at Coast Guard Aviation Repair and Supply Center; and
—Additional production capacity at a second facility.

If any of these variables are not optimal, then the schedule will not be met.

DEEPWATER PROGRAM MANAGEMENT

Question. For fiscal years 2005 and 2006, provide a detailed spend plan for program costs for ICGS Management and Government program management/ICGS.

Answer.

SYSTEMS ENGINEERING & INTEGRATION BUDGET

[Dollars in millions]

Activity	Fiscal year 2005	Fiscal year 2006
Systems Engineering:		
Performance Engineering (Measurement & Modeling) [1]	6	6
Engineering and Process Management [2]	15	16
Integration Management:		
Systems Operations Management [3]	17	17
Data Management [4]	2	2
Award Fee Pool	3	
Total	43	45

[1] *Performance Engineering.*—In accordance with Deepwater's performance-based acquisition, Performance Engineering includes the efforts required to measure the degree to which the Integrated Deepwater System achieves the overarching goals of maintaining and improving operational performance while managing total ownership costs within an aggressive baseline. Risk reduction is achieved through modeling, simulation, and analysis coupled with test & evaluation to assess the appropriate mix and capabilities of Deepwater assets to achieve the desired operational performance.

[2] *Engineering and Process Management.*—Engineering Management consists of the overarching technical management team responsible for translating Coast Guard operational and performance requirements into a cohesive Implementation Plan and managing all the technical efforts required to develop, deliver, deploy, and maintain the Deepwater assets critical to achieving the Implementation Plan. Correspondingly, Process Management is responsible for leading the identification, evaluation, implementation and improvement of Deepwater technical engineering processes deemed critical to the successful execution of the Implementation Plan.

[3] *Systems Operations Management.*—The Systems Operations Management effort includes the industry program management tasks required to direct and control all organizational functions including engineering, business management, contract management, quality management, configuration management, and data management. An Integrated Deepwater System Program Management Team (including C4ISR, Surface, Aviation, and Integrated Logistic Systems management teams) ensures effective cost control, schedule, and technical performance required to maintain the System-Of-Systems approach necessary for the Coast Guard to perform its specified missions.

[4] *Data Management.*—The Data Management effort includes tasks required to provide configuration control infrastructure for all data across the program. A program-wide Integrated Product Data Environment is utilized to integrate the efforts of geographically-separated engineering teams using a common toolset to enable rapid collaboration and sharing of consistent information.

Deepwater Program management funds are used for technical support from private sector and other government agencies not available within the Coast Guard.

GOVERNMENT PROGRAM MANAGEMENT BUDGET

[Dollars in millions]

Activity	Fiscal year 2005	Fiscal year 2006
Technical Performance Support:		
Technical Engineering Support [1]	19.1	20.1
Operational Tests and Evaluation [2]	3.8	4.0
Program Management Support:		
Financial Management [3]	3.0	3.1
Transition Support [4]	4.6	4.9
Management Support [5]	2.6	2.7
Performance Metrics/Measurement Support [6]	2.2	2.3
Information Technology [7]	2.7	2.9
TOTAL	38.0	40.0

[1] *Technical Engineering Support.*—Aeronautical, electronics and naval engineering; logistic systems, Command and Control, weapons system certification, and other expertise not available from Coast Guard resources.

[2] *Operational Tests and Evaluation.*—Navy's Commander Operational Test and Evaluation Forces is the technical advisor to the Coast Guard responsible for management of independent tests for the early review and assessment of Integrated Deepwater System asset operational performance.

[3] *Financial Management.*—Includes independent analysis and support of the Defense Contract Auditing Agency, other Defense Contract support, performance/risk management, financial systems management provided to asset level Program Management Representative Offices for independent cost analysis and pricing.

[4] *Transition Support.*—Augments Coast Guard teams for delivery of new assets, existing infrastructure changes, developing document configuration and management, graphics support, and support for training infrastructure analysis, manpower analysis, operations doctrine development, architecture analysis.

[5] *Management Support.*—Provides for program specific training, project management and outreach initiatives as recommended by Government Accountability Office.

[6] *Performance Metrics/Measurement Support.*—Modeling, simulation, and analysis of various inputs to include Total Ownership Cost, Operational Performance, and Earned Value Management Processes.

[7] *Information Technology.*—Specialized information technology to support Deepwater Program management.

MARITIME TRANSPORTATION SECURITY ACT IMPLEMENTATION

Question. On July 1, 2004, port facilities and vessels were required to submit security plans to the Coast Guard and to be in compliance with those plans. The Coast Guard has now inspected approximately 2,900 regulated facilities. The Government Accountability Office (GAO) recently concluded that it is unclear if the Coast Guard's inspection process has been effective or not. Can you describe what the Coast Guard is doing to ensure that these facilities are following through on their security plans?

Answer. The Coast Guard ensures that facilities operate in accordance with their approved security plans through annual exams and spot checks. The Coast Guard continues to work constructively with GAO to insure Coast Guard requirements and procedures are sustainable and that they make a positive impact on the security of the maritime transportation system. The requirement for an evaluation of vessel and facility security plans is one tool to reduce vulnerabilities in this critical system—the vast majority of which is owned and operated by the private sector. To ensure that regulatory and inspection frameworks continue to serve the intended objectives, regular evaluations and performance metrics are being developed to assess their effectiveness. For example, the Coast Guard plans to begin an evaluation of its facility inspection efforts in June 2005, complete the field portion of the evaluation in September 2005, and produce a final evaluation in December 2005.

Question. Last year, GAO reported that many facility and vessel owners said it would be difficult to obtain the financial resources to fully mitigate their known vulnerabilities. GAO reported that one official at a major port indicated that some security vulnerabilities were not included in its facility plan because funding was not available to address them. What is the Coast Guard doing to ensure that the inspection process is just not a "paper exercise" and one that addresses vulnerabilities?

Answer. The Coast Guard has several policies in place that provide for a meaningful inspection process and ensure facilities fully address vulnerabilities.

Prior to final Facility Security Plan (FSP) approval, Coast Guard Captains of the Port review and evaluate each submitted Facility Security Assessment (FSA), ensuring the FSPs identify and addressed all vulnerabilities. This evaluation includes an on-site survey by the Coast Guard.

After approving the FSP, the Coast Guard annually inspects each facility for MTSA compliance. The Coast Guard developed specific inspection policies to ensure that:

—The facility complies with its FSP;

—The approved FSP adequately addresses the performance-based criteria outlined in the regulations;
—The adequacy of the FSA and the Facility Vulnerability and Security Measures Summary (CG–6025); and
—Measures in place adequately address the vulnerabilities.

To carry out the inspections, qualified Coast Guard facility inspectors use a published, comprehensive inspection guide to identify deficiencies and any vulnerability not previously disclosed.

Question. With no port security grant program, how can ports know that resources are available to implement the MTSA?

Answer. DHS has administered a total of four port security grant rounds since fiscal year 2002. The Coast Guard has played a significant role in all four grant rounds, participating at every step of the process, from field recommendations to the grant awards—which have totaled over $560 million since September 11, 2001.

In 2004, Secretary Ridge designated the Office of State and Local Government Coordination and Preparedness (SLGCP) as the Department's "one-stop shop" to centralize State and local terrorism preparedness and grant administration with other emergency preparedness grant programs, including the Port Security Grant Program previously administered by the TSA. The centralization will provide better service to key stakeholders and provide a more effective overall homeland security grant program. The Coast Guard will maintain an important and active role in the port security grant process. $150 million was appropriated for fiscal year 2005 (Round 5) port security grants. A fact sheet regarding round 5 is available upon request. Additional information on the port security grant program can be found at the following internet address:

https://www.portsecuritygrants.dottsa.net/TSAdotnet/default.aspx

REQUIREMENTS GAP

Question. The Coast Guard's budget references a July 2004 "Call to Action" from the U.S. Interdiction Coordinator. That report noted that actionable intelligence has never been better but the United States is frequently unable to pursue identified interdiction opportunities. An example of this is the amount of operational hours that are available for the Coast Guard's Maritime Patrol Aircraft.

To meet the operational requirements cited in the Coast Guard's MPA requirements study, the Coast Guard would have to double the amount of maritime patrols from the current capability of 32,000 hours. Your budget includes an increase of only 1,500 maritime patrol hours for homeland security, counter-drug, and other mission areas. Why does such a large gap in requirements exist and what will it take to close it?

Answer. The Coast Guard fixed wing requirements were determined by calculating the post-September 11 mission needs above the 1998 Coast Guard multi-mission baseline. The 1998 baseline was 44,400 hours. The additions are: 5,139 hours for counter-drug (CD) hours based on Joint Inter-Agency Task Force South analysis of the Department of Defense and multi-national drawdown in CD forces; 18,195 hours for maritime security long range surveillance under moderate, high and imminent threat periods; and 285 hours for Coast Guard Strike Force and Maritime Safety and Security Team transport. Given that 32,400 flight hours are available from Coast Guard fixed wing aircraft in fiscal year 2005, this leaves a gap of 34,454 hours.

The Coast Guard's fiscal year 2006 budget includes several initiatives to help mitigate the current Maritime Patrol Aircraft (MPA) shortfall:

—$16.5 million is requested for C–130H augments, providing an additional 1,500 annual C–130H MPA flight hours. Funding will also provide for dedicated aviation sensor personnel and enhanced sensors to improve effectiveness in high-threat zones, and permanently establish forward operating and logistics support for MPA operating in the Central/South American region to maximize time "on station" and reduce aircraft downtime due to unscheduled maintenance.
—$12.6 million is requested for 1200 additional annual operations flight hours for C–130Js to conduct proficiency training and logistics flights—freeing up missionized C–130Hs to conduct MPA missions.
—$5 million is requested to continue the missionization of the 6 C–130Js, through operation of the Aircraft Project Office, which are estimated to be completely missionized by 2008.
—$8.7 million is requested to staff and support the first two CASA aircraft in advance of delivery and full operating capability anticipated in 2007.

The MPA gap will likely persist until the Deepwater system (including the CASAs, C–130s, and unmanned aerial vehicles) is fully built out.

Question. What other major Coast Guard assets have a gap between capabilities and mission requirements?

Answer. The significant capability gaps faced by the Coast Guard's major assets in the post-September 11 environment were the catalyst for the Deepwater Performance Gap Analysis and subsequent Mission Need Statement and the revised Deepwater Implementation Plan. These gaps are quantified both under capability—the attributes of individual assets, and capacity—force structure/fleet size. The following table depicts the capabilities and capacity for the Deepwater fleet to begin to close these gaps.

In addition to the MPA gap, a capacity gap exists with the patrol boat fleet. Considering available 110-foot and 123-foot patrol boats and 179-foot patrol coastals on loan from the U.S. Navy, total patrol boat available hours reached it lowest point of approximately 75,000 in 2004. This is considerably lower than the 1998 baseline of approximately 100,000 hours, and is a result of having cutters deployed to Operation Iraqi Freedom, and cutters out of service for the 110–123 foot conversion program. With the advancement of the fast response cutter design and construction, the Coast Guard should reach the 1998 baseline again between 2013 and 2015.

Asset	Original Mission Needs		Revised Mission Needs	
	Fleet Size	Capabilities	Fleet Size	Capabilities
National Security Cutter (NSC)/Maritime Security Cutter, Large (WMSL)	8	Deepwater Interoperability Basic CG Command and Control (C2) Feed Forward Looking Infrared	8	DHS/DOD/Rescue 21 (R21) Interoperability Remote/Integrated Anti-Terrorism/Force Protection (AT/FP) Weapons Redundant/Hardened/Improved C2 Underwater Detection
Offshore Patrol Cutter (OPC)/Maritime Security Cutter, Medium (WMSM)	25	Deepwater Interoperability 22 kt Speed Standard Flight Deck	25	DHS/DOD/R21 Interoperability CG COP Connectivity Integrated Electo-Optical/Infrared System
	.....	Threat Receiver 30mm Gun Manual Small Arms	.....	Chemical, Biological, Radiological, Nuclear & Explosive (CBRNE) Detection Enhanced Maritime Patrol Surveillance Capability Nation-wide DHS Strategic Lift
Fast Response Cutter (OPC)/Maritime Patrol, Coastal (WPC)	58	Deepwater Interoperability 30mm Gun Baseline C4 Suite Threat Receiver 20-yr Steel Hull	58	DHS/DOD/R21 interoperability Remote Weapons & AT/FP Suite Redundant, Hardened C4 Defense Survivability 40-yr Composite Hull CBRNE Detection & Defense Underwater Detection
Short Range Prosecutor (SRP)	42	Deepwater Interoperability	33	DHS/DOD/R21 Interoperability
Long Range Interceptor (LRI)	82	Deepwater Interoperability	91	DHS/DOD/R21 Interoperability
Long Range Surveillance Aircraft (LRS)/ HC–130H/J	6	Deepwater Interoperability Basic CG C2 Feed Forward Looking Infrared	22	DHS/DOD/R21 Interoperability CG COP Connectivity Integrated Electo-Optical/Infrared System CBRNE Detection Enhanced Maritime Patrol Surveillance Capability Nation-wide DHS Strategic Lift
Multi-Mission Cutter Helicopter (MCH)/HH–65C	93	Deepwater Interoperability	95	DHS/DOD/R21 Interoperability CG COP Connectivity CBRNE Detection Airborne Use of Force Vertical Insertion/Delivery

Medium Range Surveillance Aircraft (MRS)/CASA CN–235	35	Deepwater Interoperability	36	DHS/DOD/R21 Interoperability CG COP Connectivity Integrated Electo-Optical/Infrared System CBRNE Detection
Medium-Range Recovery Helicopter (MRR)/MH–60T	42	Deepwater Interoperability	42	DHS/DOD/R21 Interoperability CG COP Connectivity Integrated Electo-Optical/Infrared System CBRNE Detection Airborne Use of Force Vertical Insertion/Delivery
Vertical Take-off & Landing UAV (VUAV)	69		45	CBRNE Detection
High Altitude & Endurance UAV (HAEUAV)	7		4	

PORT SECURITY ASSESSMENTS

Question. In the fiscal year 2003 Supplemental, Public Law 108–11, Congress appropriated $38 million to conduct vulnerability assessments at all tier I strategic seaports. Of that amount, $16.8 million remains unobligated. Why hasn't this funding been spent?

Answer. Prior to enactment of Public Law 108–11, the Coast Guard received supplemental funding and was able to conduct Port Security Assessments (PSAs) at 13 of the 55 strategic ports. The average cost of these assessments was $900,000 per port. The $38 million appropriation was to complete remaining port assessments based on this per-port average.

In response to various maritime security initiatives, such as the Maritime Transportation Security Act of 2002, the Coast Guard revised the PSA methodology to ensure that the PSAs provided the greatest value to the port without being redundant to the other initiatives and programs. This updated methodology resulted in a reduction of costs from $900,000 to approximately $300,000 per port.

As of September 14, 2005, the Coast Guard has expended $22.9 million for the completion of PSAs of the Coast Guard's 55 militarily and economically strategic ports, as well as for important port security initiatives such as special technical assessments, development of a Geographic Information System (GIS) viewer, Coast Guard participation in the Comprehensive Review of nuclear power plants, and PSA Program operational costs. The remaining $16.6 million will be expended during the remainder of fiscal year 2005 and 2006 to continue refining port security assessments and our knowledge of port-specific vulnerabilities through specific technical or infrastructure assessments (bridges, tunnels, dangerous cargo, etc.). This additional work is critical to address needs that were identified in the course of the initial port assessments. It will provide important amplifying information to Coast Guard Captains of the Port and the Area Maritime Security Committees allowing them to address effectively port-specific vulnerabilities that have been identified.

Question. How many assessments of tier I ports have been completed to date and what is the schedule to complete all Tier I ports?

Answer. All Tier I PSAs are complete. The Coast Guard has completed PSAs at each of the previously identified 55 militarily and economically strategic U.S. ports, of which "Tier I" ports are a subset.

PORT SECURITY ESTIMATES

Question. Last year, in response to a question for the record on port security, the Committee was told that Department of Homeland Security spending on port security increased by $224 million (13 percent) in the President's Budget, from $1,661 million in 2004 to $1,885 million in 2005. Within the 2005 total is $1,675 million for Coast Guard port, waterway, and coastal security activities, including over $100 million for expenses related to the Maritime Transportation Security Act (MTSA). How was that funding level determined?

Answer. The $1,675 million for Coast Guard Ports, Waterways, and Coastal Security (PWCS) activities in fiscal year 2005 was incorrectly stated in last year's question. The 2005 operating expense budget estimate for PWCS activities estimated in the Coast Guard's 2005 Budget congressional justifications as $1,501 million. The Coast Guard develops estimates of mission-specific spending using an activity based Mission Cost Model. The $101 million increase to implement MTSA attributable to PWCS was included in the $1,501 million estimate.

PORT SECURITY GRANT PROGRAM

Question. The Coast Guard authorization Act for 2005, which was signed into law by the President on August 9, 2004, authorized $35 million for the Secretary to fund pilot programs and award grants to investigate new methods and technologies to better secure our ports. The law specifically cites the need to examine new technologies such as those that can accurately detect explosives, chemical or biological agents, and nuclear materials. The law calls for the examination of new methods for securing our ports such as the use of satellite tracking systems and tools to mitigate the consequences of a transportation security incident. The fiscal year 2006 request does not include funding for this program. What intelligence led the Coast Guard to believe that such a program was unnecessary?

Answer. The Coast Guard is aggressively moving to implement new technologies in order to better secure our ports. Rather than pilot programs or grants, the Coast Guard believes it more prudent in the near term to expend limited resources on the deployment of important proven technologies while other DHS components responsible for development of cross-cutting technologies and private sector grant and re-

search programs administer pilot and grant programs, notably the S&T Directorate and SLGCP. S&T, in particular, has a wealth of research and development expertise as well as an active university research program to pursue technology enhancements across all homeland security requirements. Concurrently, SLGCP is overseeing the administration of a port security grant program that has awarded over $560 million in port security grants already, and will award another $150 million in fiscal year 2005.

In the near term, the Coast Guard is focused on enhancing Maritime Domain Awareness (MDA). MDA is defined as "the effective understanding of anything associated with the global maritime environment that could impact the security, safety, economy or environment of the United States." Effective MDA is a critical enabler to national maritime security strategies and supports the full range of Coast Guard missions.

COVERT SURVEILLANCE AIRCRAFT

Question. What is the Coast Guard's definition of a "covert surveillance aircraft"?

Answer. The 2005 DHS Appropriations Act conference report defines the manned covert surveillance aircraft as a "medium to short range, fixed wing surveillance aircraft." In the context of the Coast Guard's Manned Covert Surveillance Aircraft (MCSA) acquisition project, "covert" is defined as "the capability to operate quietly and surreptitiously enough to enable the surveillance, detection, classification and identification of a maritime target without the target's inhabitants becoming aware of the aircraft's presence."

Question. How will a covert surveillance aircraft serve the Coast Guard's mission?

Answer. The Coast Guard is developing the operational requirements documents that will define the missions and operating parameters for a manned covert surveillance aircraft. The Coast Guard is also examining how this aircraft will fit into the Deepwater system, given that the Deepwater implementation plan accounts for the service-standard fixed, rotary wing and unmanned aircraft necessary to meet projected Coast Guard mission needs documented in the revised Mission Needs Statement.

Question. How much does the Coast Guard estimate the cost of a covert surveillance aircraft to be?

Answer. The rough order of magnitude acquisition cost of a fully missionized, FAA-certified manned covert surveillance aircraft is estimated to be $8 million.

Question. What is the timeline for acquiring a covert surveillance aircraft or aircrafts for operational use?

Answer. The procurement timeline is currently being constructed with the Manned Covert Surveillance Aircraft acquisition team. The following table provides the best estimate of initial operating capability (IOC).

Operational Requirements Document Written & Approved	July 2005
Release of Request for Proposal	September 2005
Aircraft Award	January 2006
Airworthiness Certification Test/Evaluation Commencement	January 2007
Initial Operating Capability	January 2006

Question. Are there existing platforms available on the commercial market that would meet the Coast Guard's specifications for a covert surveillance aircraft? If so, please describe them.

Answer. Currently, the Coast Guard is developing the operational requirements and specifications for the Manned Covert Surveillance Aircraft. Once these are defined and approved, the Coast Guard will conduct a formal market survey and or request for proposal to determine the availability of any suitable aircraft in the commercial market that meets its requirements.

AUTOMATIC IDENTIFICATION SYSTEM

Question. The Coast Guard has obligated $7.5 million to a contract with a commercial low earth orbit satellite communications provider for the installation of AIS capability on a concept validation satellite and design for installation on future satellites. What type of coverage does this provide to the Coast Guard?

Answer. The deployment of a concept validation payload aboard a commercial low earth orbit satellite is a prototype for the receipt of AIS signals via satellites from vessels within 2000 nautical miles of the U.S. coast.

Question. The AIS budget provides for approximately $30 million per year over the next five fiscal years (including fiscal year 2006). Could this acquisition program be accelerated if additional funding became available?

Answer. The Coast Guard's fiscal year 2006–2010 Capital Investment Plan calls for project completion in 2011; however, the project could be completed sooner if additional funding is provided.

COAST GUARD SUPPORT OF NSF RESEARCH OPERATIONS IN THE POLAR REGIONS

Question. The budget request for the National Science Foundation includes $48 million in budget authority to operate and maintain the 399 foot Polar Icebreakers. This amount does not include funding such as extraordinary maintenance costs. In fiscal year 2005, these extraordinary maintenance costs are estimated to be $18 million. The budget indicates that a Memorandum of Understanding (MOU) is being discussed to address these additional costs. What is the status of the MOU between the National Science Foundation (NSF) and the U.S. Coast Guard?

Answer. The Coast Guard and NSF are currently negotiating to conclude an MOU for fiscal year 2006.

The $48 million NSF budget authority represents the base funding to operate and maintain the 399 foot POLAR STAR and POLAR SEA and the 420 foot HEALY. The MOU will reflect an agreement between NSF and Coast Guard for NSF to pay for all personnel, maintenance and operational funds necessary to manage the polar icebreaking program.

The Administration plans to maintain current polar icebreaker fleet capabilities at least until a new national polar icebreaker requirements policy decision is made.

Question. Please provide a historical breakdown, by fiscal year, of the costs to support the NSF's scientific and operational programs in the Polar Regions, including maintenance costs, and how much the NSF reimbursed for those costs in each fiscal year.

Answer. In recent years, the Coast Guard icebreaker fleet has devoted, on average, 82 percent of its operational time in support of the NSF. The chart below attributes NSF's percentage of operational time to the total annual funding for the icebreakers (including maintenance costs).

The following table provides a historical breakout of Coast Guard polar icebreaking support costs, those costs attributable to NSF activities, and the amounts reimbursed by NSF to the Coast Guard per the MOA between the two agencies.

Fiscal year	Reimbursement Amount from NSF	Total Costs required to support cutters [1]	Percent Operational time devoted to NSF	Cost to support NSF programs
1999	$2,711,732	$31,397,056	76	$24,004,075
2000 [2]	2,145,242	40,971,438	80	32,777,150
2001	4,966,672	41,899,046	64	26,839,661
2002	5,961,684	49,195,000	93	45,643,381
2003	8,165,647	50,501,309	91	45,925531
2004	12,422,190	57,585,544	89	51,189,137

[1] Note: Costs include actual unit level operating and maintenance costs, fuel costs, depot level maintenance costs, and personnel costs for the salaries and benefits attributable to the people assigned to the cutters. These costs have grown to exceed budgeted amounts due to extraordinary maintenance costs required to sustain the polar icebreaking fleet. The President's fiscal year 2006 budget proposes transfer of the Coast Guard's base funding (using budgeted amounts) to support operation and maintenance of these cutters.

[2] Reflects the addition of the HEALY as the third Coast Guard icebreaker.

Question. If a Memorandum of Understanding is not reached and the NSF decides to contract out for their icebreaking needs in the polar region, would the Coast Guard need to maintain the Polar Sea and the Polar Star icebreakers?

Answer. On August 8, 2005, the Coast Guard signed an MOU with NSF to ensure that the polar icebreaking fleet will be operated and maintained in fiscal year 2006.

Question. If so, what functions would they serve and what would be the costs in fiscal year 2006?

Answer. The polar class icebreakers (POLAR SEA and POLAR STAR) have been and will continue to primarily support the U.S. Antarctic Program re-supply effort (Operation Deep Freeze) each year. Due to Antarctic ice conditions, the age of the vessels and the breakers' increasing maintenance needs since 2001, these two vessels are no longer able to support simultaneously the U.S. Antarctic Program. Pending additional funding from the NSF in fiscal year 2006, POLAR SEA will continue the second year of a 2-year maintenance availability to ensure readiness for the Operation Deep Freeze 2007 deployment to Antarctica. POLAR STAR is currently scheduled to support the 2006 Operation Deep Freeze mission. HEALY is scheduled to support Arctic research, typically lasting from May to November of each year. The fiscal year 2006 base funding and overall costs are outlined below:

FISCAL YEAR 2006 COAST GUARD POLAR ICEBREAKER BASE FUNDING

Projected costs AFC	Cost center HEALY	POLAR SEA	Fiscal year 2006 POLAR STAR	Total
Training & Recruiting	$210,512	$355,244	$355,244	$921,000
Military Personnel	5,936,630	9,547,685	9,547,685	25,032,000
Depot Level Maintenance	4,498,926	4,493,037	4,493,037	13,485,000
Operating and Maintenance	3,586,000	2,000,000	2,000,000	7,586,000
Central Accounts	109,000	183,500	183,500	476,000
Grand Total	14,341,068	16,579,466	16,579,466	47,500,000

FISCAL YEAR 2006 PROJECTED COSTS REQUIRED TO SUSTAIN POLAR ICEBREAKER FLEET ABOVE THE BASE FUNDING LEVEL

Projected costs AFC	Cost center HEALY	POLAR SEA	Fiscal year 2006 POLAR STAR	Total
Depot Level Maintenance	$7,100,000	$9,700,000	$500,000	$17,300,000

Question. If not, what would be the cost for the Coast Guard to mothball or dispose of the two icebreakers?

Answer. The Coast Guard estimates that the cost to mothball or dispose of each Polar Class Icebreaker is $750,000 per hull, for a total of $1.5 million.

The estimated personnel transfer cost if the two icebreakers are decommissioned is $700,000.

Question. What are the long-term costs to maintain the Coast Guard's Polar Icebreakers?

Answer. The two heavy polar icebreakers are nearing the end of their service lives and require major systems overhauls to continue to operate in a cost-effective manner. The Coast Guard has not developed detailed analyses of the costs associated with the long-term costs of recapitalizing the heavy polar icebreaking fleet. As the national needs for heavy polar icebreaking are more thoroughly studied by the National Academies of Sciences (NAS), the Coast Guard will inevitably be involved in developing long-term cost estimates for heavy polar icebreaking.

Since the Healy medium-duty polar icebreaker is a relatively new vessel, there are no significant long-term maintenance costs above the budgeted base amounts for that ship.

Question. What efforts are underway to fund a replacement vessel or overhaul one or more of the existing vessels to support the long-term needs of the scientific community?

Answer. There are no plans to replace or overhaul CGC HEALY, which was commissioned in 2000.

In accordance with the fiscal year 2005 Homeland Security Appropriations Bill Conference Report, the NAS will be conducting a polar icebreaker study, with an interim report expected during November 2005 and completion of the final report anticipated during July 2006. The NAS study report could be used as the basis for an update of the 1990 Presidential Decision Determination on national polar icebreaker requirements policy.

Question. What would the cost be and the amount of time necessary to acquire a new polar icebreaker?

Answer. Initial rough estimates indicate that one new polar icebreaker, with the equivalent heavy icebreaking capabilities as the Polar Class icebreakers, would cost approximately $600 million and would require 6 years to construct.

Question. The Coast Guard is absorbing roughly $9 million in fiscal year 2005 to meet key milestones in the maintenance of the Polar Sea. Is critical maintenance in other areas being delayed or canceled to meet the needs of the Polar Sea?

Answer. Yes, the $9.2 million for extraordinary maintenance of the POLAR SEA will be absorbed within the Coast Guard's fiscal year 2005 maintenance funds, requiring deferral of critical maintenance in other areas, such as replacement of aging and obsolete subsystems onboard Coast Guard legacy cutters.

Question. If so, please describe those delays and the impact they will have on the Coast Guard fleet.

Answer. As the end of fiscal year 2005 approaches, and the level of fleet-wide unscheduled maintenance activity becomes clearer, specific maintenance activities will

be identified for deferral by Coast Guard maintenance managers as they shift resources to deal with their most immediate fleet maintenance challenges.

Question. Section 888 of Public Law 107–296 ensures that Coast Guard "functions and capabilities be maintained intact and without significant reduction." Under what authority does the proposal to transfer funding for icebreaking operations to the NSF fall under?

Answer. Subsection 888(c) of the Homeland Security Act of 2002 provided that: "the authorities, functions, and capabilities of the Coast Guard to perform its missions shall be maintained intact and without significant reduction after the transfer of the Coast Guard to the Department, except as specified in subsequent Acts."

The proposed shift of appropriations for polar icebreaking, if enacted, does not remove any of the authorities, functions, or capabilities of the Coast Guard. Since NSF and the Coast Guard have a signed MOU ensuring funding for the icebreaking program in fiscal year 2006, the Coast Guard will continue to perform its polar icebreaking mission. Furthermore, the proposed shift of appropriations, if enacted, would be the result of a "subsequent act" of Congress, in the terms of Subsection 888(c).

RECRUITING

Question. What is the Coast Guard's goal for recruiting active duty personnel in fiscal year 2006? Provide a chart showing the total number of recruits in each of the past 10 years for active duty personnel and reserves and compare them against the Coast Guard's targets for those years.

Answer. The following tables show the total number of Coast Guard active duty and reserve recruits in each of the past 10 years compared with the Coast Guard's targets for those years.

COAST GUARD ACTIVE DUTY RECRUITING

Year	Targets	Accessed
1996	3,300	3,299
1997	3,900	3,697
1998	4,464	3,962
1999	4,150	4,159
2000	4,700	4,721
2001	4,300	4,332
2002	4,800	5,169
2003	4,475	4,488
2004	3,800	3,809
2005	4,110	[1] 4,110
2006	[1] 4,200	[1] 4,200

[1] Projected.

COAST GUARD RESERVE RECRUITING

Year	Targets	Accessed
1996	350	229
1997	430	303
1998	1,313	554
1999	900	801
2000	900	692
2001	700	424
2002	718	585
2003	1,150	880
2004	940	911
2005	950	[1] 800
2006	[1] 900	[1] 900

[1] Projected.

C–130JS

Question. In March, the Coast Guard placed interim limitations on the HC–130H 1500 series aircraft. What is the status of these restrictions?

Answer. The HC–130H 1500 series aircraft are operationally restricted/limited based on potential cracking in the center wing box based on effective wing age. The

restrictions on the five Coast Guard 1500 series aircraft are similar to restrictions imposed on United States Air Force aircraft of similar vintage and use rate. The restrictions are designed to limit wing loading by limiting fuel, cargo and airspeed under certain conditions. These restrictions will remain in place until Lockheed Martin Aero (LMA) Service Bulletin (SB2) is developed and the required inspections are completed. SB2 is expected on May 30. Each aircraft inspection will take approximately 1 month to complete. If serious structural cracking is found during inspections, the Coast Guard will determine whether to refurbish the affected aircraft to keep them in service well into the future or if there are other alternatives.

Question. What impact have these restrictions had on the Coast Guard?

Answer. The restrictions currently impact only the five 1500-series C–130s at Coast Guard Air Station Elizabeth City and have resulted in some degradation of the unit's ability to perform long-range search and rescue, maritime patrol, logistics and International Ice Patrol missions. These operational restrictions are based on reduced fuel and cargo loads similar to those imposed on United States Air Force aircraft of similar vintage and use rate. The restrictions reduce the maximum endurance of the aircraft from 12 to 7.5 hours, reduce the maximum cargo capacity from 45,000 to 10,000 lbs, require slower airspeed when in the vicinity of turbulence and require greater fuel reserves. These restrictions have been mitigated by incorporating more refueling stops and or using newer 1700-model C–130s without restrictions.

Question. What are the Coast Guard's plans to remedy the structural problems, including necessary funding?

Answer. There are no known structural problems to be remedied. The 1500 series aircraft are operationally restricted/limited based on the potential of cracks in the center wing box based on effective wing age. LMA is currently developing the procedures to inspect the wings to determine if cracks exist. If inspections find no evidence of structural cracking, the operational restrictions will be adjusted or removed. If serious structural cracking is found during inspections, the Coast Guard will determine whether to refurbish the affected aircraft to keep them in service or if there are other alternatives. Cost estimates to effect necessary repairs will be based on the results of the inspections.

SIPRINET

Question. The Coast Guard is in the process of increasing its SIPRNET presence to include all of its major shore side operational units (Areas, Districts, Sectors, & Air Stations). Approximately half of the planned shore side Coast Guard units (80 out of 156) currently have SIPRNET connectivity. What is the funding level for this activity in fiscal year 2006?

Answer. The Coast Guard SIPRNET Program is fiscal year 2006 base of funds is $9.5 million. This includes funding for recurring circuit costs, contract labor costs, new installations, and equipment recapitalization.

Question. What is the current schedule to provide connectivity to the remaining units?

Answer. The Coast Guard is currently planning to fund the installation of 23 new sites during fiscal year 2006. The Coast Guard anticipates completing SIPRNET installations at all 152 sites by fiscal year 2009.

Question. Could the schedule be accelerated if additional funding became available in fiscal year 2006?

Answer. Additional funding in fiscal year 2006 would not accelerate the installation schedule. The installations are currently scheduled at maximum install rate due to the time required to build the facilities and installation contractor resource capabilities.

MARITIME SECURITY CUTTER—LARGE OPERATIONAL COSTS

Question. The Coast Guard is expecting the first WMSL to be delivered in May 2007. Please provide a spend plan and timeline related to the funding necessary for pre-commissioning familiarization and training for core personnel.

Answer. The timeline for pre-commissioning training and familiarization is as follows:

—*Phase I: Winter/Spring 2005.*—Five crewmembers reported to Pascagoula for pre-arrival training, ship engineering familiarization, and doctrine development. Cost: $151,352

—*Phase II: Summer/Fall 2006.*—96 crewmembers report to Alameda (the ship's homeport) to conduct pre-arrival training, which is provided at various government and commercial facilities around the country. Following pre-arrival train-

ing, these crewmembers will proceed to Pascagoula for pre-commissioning familiarization. Cost: $1,830,816

—*Phase III: Winter/Spring 2007.*—Remaining 61 crewmembers report to Alameda then immediately proceed to Pascagoula for pre-commissioning familiarization. Cost: $1,063,930

—*May 2007.*—First National Security Cutter/Maritime Security Cutter Large (WMSL) is delivered to the Coast Guard.

The travel and subsistence cost for crewmembers to complete the initial pre-arrival and pre-commissioning training is estimated at $3.1 million.

RESEARCH & DEVELOPMENT

Question. Section 888 of Public Law 107–296 ensures that Coast Guard "functions and capabilities be maintained intact and without significant reduction." Under what authority does the proposal to shift Cost Guard R&D functions to the S&T Directorate fall under?

Answer. Subsection 888(c) of the Homeland Security Act of 2002 provided that: "the authorities, functions, and capabilities of the Coast Guard to perform its missions shall be maintained intact and without significant reduction after the transfer of the Coast Guard to the Department, except as specified in subsequent Acts."

The proposed shift of appropriations for Research, Development, Test and Evaluation from the Coast Guard to the S&T directorate, if enacted, would be the result of a "subsequent Act" of Congress, in the terms of Subsection 888(c).

Question. How would the proposed transfer improve the ability of the Coast Guard to accomplish its missions?

Answer. The consolidation of Research and Development (R&D) funding at the Department level will maximize effectiveness of R&D activities across the Department by minimizing redundancies. Through the Coast Guard portfolio manager at S&T, the Coast Guard will continue to develop and provide homeland and non-homeland security research requirements which support all of the Coast Guard's homeland and non-homeland mission programs.

ATTRITION RATE

Question. What is the current attrition rate for Secret Service agents and Uniformed Division Officers?

Answer. In fiscal year 2004, the attrition rate for special agents was 6.28 percent, and for Uniformed Division officers 7.6 percent. The Secret Service expects that the attrition rate for fiscal year 2005 for special agents will be 5.2 percent, and for Uniformed Division officers 8.5 percent.

OVERTIME RATE

Question. What is the current monthly overtime rate for Secret Service agents?

Answer. The current average monthly overtime rate for Secret Service agents is 71 hours.

PAY INCREASE

Question. The budget includes funding for a 2.6 percent pay increase for Secret Service employees in 2006, but the Administration requested a 2.1 percent across the board pay increase for Federal employees. Why is the Secret Service budgeting for a higher pay increase?

Answer. The Secret Service's fiscal year 2006 budget includes funding for a 2.3 percent pay increase for Federal employees. This is the same percentage increase proposed by the Administration.

Question. What is the cost difference between a 2.1 percent pay increase and a 2.6 percent pay increase?

Answer. A 2.1 percent pay increase would require $11,752,000, and a 2.6 percent pay increase would require $14,550,000, a difference of $2,798,000. The Secret Service request was $12,871,000 or 2.3 percent.

WHITE HOUSE MAIL

Question. The budget includes $16.365 million to process White House mail. What is the status of the Department's efforts to develop a long-term plan for a fully operational White House Mail facility?

Answer. In the summer of 2004, the U.S. Secret Service and the General Services Administration (GSA) initiated the planning of a permanent White House mail facility.

The stakeholders utilized two previous studies in order to begin their effort. In 2003, the Secret Service commissioned Science Applications International Corporation (SAIC) to develop a full-scale mail screening facility in concept. In addition, GSA conducted a site selection study in which they identified four feasible locations in the Washington, D.C. metropolitan area for a White House mail facility.

In October 2004, GSA procured the services of HDR, an architectural engineering and consulting firm, to complete a Program Development Study (PDS). The PDS, which was completed in February 2005, reflects the efforts of the team to define the feasibility, analyze needs, prepare cost analysis and program requirements for the program. A mail screening facility proposal was defined by the PDS. Three sites located at the Anacostia Naval Annex were selected as most feasible. The PDS estimated the cost for construction at $33.5 million.

Since the completion of the PDS, the development team has worked closely with GSA to identify a potential future site for the White House mail screening facility. GSA is working with the Navy Real Estate Office to assess the availability of property at the Anacostia Naval Annex, in Washington, D.C. adjacent to other White House support facilities for this purpose. Upon identification of available Federal property, GSA will conduct environmental and design studies of the potential site. This information will be used to determine the GSA facility acquisition plan (lease/build) and project the new facility's operational costs.

Question. What is the percentage of mail addressed to the White House that doesn't reach its destination?

Answer. For the 14-month period beginning in March 2004 and ending April 2005, the White House mail screening facility received approximately 1,730,000 pieces of mail, flats or parcels. Of these, 288,800 items (or 16 percent) were classified as junk mail and, therefore, not processed at the facility. Of the remaining 1,441,200 processed mail pieces, 1,441,000 (or 99.9 percent) pieces were delivered to the complex.

The two hundred pieces of mail (or less than 1 percent) not delivered to the complex were identified by the facility as containing an unknown substance or an overt threat and were referred to the Secret Service Intelligence Division for investigation. In addition, 29 referrals were made to Secret Service field offices due to items received at the facility and two arrests were made.

EMERGENCY RESPONSE FUND

Question. The latest report (date) from OMB on the status of the $40 billion Emergency Response Fund, enacted 3 days after 9/11, shows that the Secret Service has an unobligated balance of $6 million. Why have the funds not been used and what are your plans for the unobligated funds?

Answer. As of October 2004, the Secret Service had no unobligated balance from the Emergency Response Fund.

NATIONAL RESPONSE PLANNING

Question. DHS has recently released the National Incident Management System Plan, the Nation Preparedness Goal and begun the roll out of the National Response Plan which will better guide the spending of Federal resources like the over $11 billion Congress has appropriated for first responders programs. With this additional guidance, what changes have you seen/do you expect to see in the local requests for projects that will prevent wasteful spending?

Answer. The National Incident Management System (NIMS) integrates effective practices in emergency preparedness and response into a comprehensive national framework for incident management. The NIMS will enable responders at all levels to work together more effectively to manage domestic incidents no matter what the cause, size or complexity. The Department is requiring that states and territories begin work on compliance with the NIMS as part of their fiscal year 2005 grant funding.

The National Response Plan (NRP) establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector—and integrates them into a unified structure. It forms the basis of how the Federal Government coordinates with State, local, and tribal governments and the private sector during incidents.

The National Preparedness Guidance, issued on April 27, 2005, addresses the implementation of the NIMS and the NRP, as one of the overarching national priorities. DHS is now beginning to work with states, territories, and urban areas to update their existing State and urban area homeland security strategies to bring them

into alignment with the seven national priorities. This alignment with the national priorities will enable States and territories to continue expending funds in accordance with the goals and objectives already outlined in the strategies. With this, DHS expects a greater emphasis on training and exercises to further implement the NRP and NIMS within the States and territories. Historically, there has been a higher trend towards the purchase of specialized equipment, but DHS believes that the States are undertaking training and exercise programs that typically require longer-term planning.

Question. How have the State and local entities reacted to the changes?

Answer. State and local entities have had many questions about the publication of all three of these documents. Understandably, they do not always clearly understand the intent of the documents and how they are related to the grant funding that they receive. Likewise, they are concerned about the resources they will need at the State level to ensure compliance. Anticipating such concerns, DHS created on-line training materials through FEMA/USFA's Emergency Management Institute and National Fire Academy's Distance Learning Programs that cover both NIMS and the NRP. To date, more than 200,000 personnel have completed these training courses. In order to further articulate these requirements, the Department has scheduled several rollout conferences for the NIMS and NRP across the country to educate the State and local stakeholders. The NIMS Integration Center (NIC) is responsible for orchestrating NIMS implementation and NIMS compliance. Through training, exercises, and technical assistance, the NIC is working to ensure that our state, local, and tribal partners understand NIMS and take the appropriate steps to implement it in their communities. In addition to the NIMS and NRP outreach, the Office for Domestic Preparedness (ODP), within SLGCP, has scheduled three additional meetings on the National Preparedness Guidance so that States and territories understand the imbedded requirements. We also are offering technical assistance packages that are customized to each State and territory. ODP is committed to providing additional education and outreach to our grantees as we move forward in implementing the seven national priorities codified in the National Preparedness Guidance.

SLOW PACE OF GRANT DISTRIBUTIONS

Question. On October 18, 2004, the President signed into law the fiscal year 2005 Homeland Security Appropriations Act. The majority of the grants funds have just recently been made available for application this month: 6 months since the Act was signed into law. Rail security funds were made available on April 5, 2005. Transit security funds were also just made available on April 5, 2005. Port security funds, as of April 20, 2005, still have not been made available for application. The State Homeland Security Grant Program is the only program that has awarded funding and that is because the Congress required it by law. None of the other fiscal year 2005 homeland security grant funds have actually been distributed.

Why is it taking so long to get the money out the door?

Answer. The responsibility for most non-aviation grant programs was transferred from the TSA to SLGCP during fiscal year 2004. This resulted in a transition period while programs and staff adapted to different processes and new automation. More importantly, the Department has used this time to work with Federal partnering agencies and applicable state, local, and private sector stakeholders to redesign these programs to include a more risk-based approach to allocation of funding that aligns with Administration priorities as described in Homeland Security Presidential Directive (HSPD)-8 and the recently released National Preparedness Goal. The Department is committed to awarding grants earlier in the year while maintaining effective oversight.

Question. What steps are being taken to expedite the process?

Answer. Completion of the programmatic redesign process coupled with automation of the application submission, reporting, and payment processes for these programs will result in greatly enhanced processing capabilities for future program funding. In addition, SLGCP has established the Transportation Infrastructure Security Division to manage these programs. The Division is in the process of filling remaining vacancies and consequently will be in a greatly strengthened position for management and administration of future grant programs.

Question. When will funding be awarded for Intercity Passenger Rail Security, Transit Security, Intercity Bus Security and Port Security grants?

Answer. The current schedule for each program is as follows: Intercity Passenger Rail Security Program—awarded July 18, 2005; Transit Security Grant Program—awarded July 15, 2005; Intercity Bus Security Grant Program—first round of awards were awarded on August 9, 2005, and the final round of awards will be

awarded on September 30, 2005; Port Security Grant Program—awarded September 1, 2005.

Question. As part of your Department review, will you commit to expediting the grant making process so that money that is supposed to make Americans safer does not sit in the Treasury in Washington, DC?

Answer. The Department takes its responsibility very seriously for protecting Americans and the critical transportation infrastructure they depend on. As stated previously, the recent redesign of these programs, coupled with the newly instituted SLGCP Transportation Infrastructure Security Division and automation of the application, reporting, and payment processes for these programs will result in significantly enhanced capabilities relative to the management and administration of these programs. In addition, SLGCP is also in the process of establishing an Office of Grants Operations that will further streamline financial management activities associated with these grants.

PORT/RAIL/TRANSIT

Question. According to the American Public Transportation Association, there are approximately 9.6 billion transit trips annually and people use public transportation vehicles over 32 billion times each workday. This is more than 16 times the number of aviation passengers, and yet the Department continues to spend less than 10 percent of its transportation security resources on non-aviation security. The President's Budget Request proposes that individual grant programs for port, rail/mass transit, bus, and truck security grant programs be eliminated and collapsed into a new grant program called a "Targeted Infrastructure Protection Grants" program. Because none of the previous individually appropriated grant programs are specified in this new account—ports will compete against rail and mass transit, and other infrastructure for $600 million. For mass transit security alone, the American Public Transportation Association estimates a need for $6 billion in transit security. Not only does this insufficient request show a lack of support for modes of transportation other than air travel security but it further frustrates the officials responsible for securing people's safety on these modes by pitting them against each other for scarce resources. We currently spend $5 billion on aviation security. This proposal continues a disturbing pattern by the Department of focusing on the last battle—aviation security—and less on non-aviation modes of transportation.

How does the agency really expect that this request furthers the mission of homeland security when we are only as strong as our weakest link?

Answer. Enhancing the security of the Nation's critical infrastructure, including transportation, continues to be a high priority for the Department, which is why the Department proposed the development of a Targeted Infrastructure Protection (TIP) Program. This program would consolidate Port Security, Rail/Transit Security, Intercity Bus Security, and Trucking Industry Security grant programs into a single larger program. Because it is unrealistic to anticipate infrastructure threats and protection needs nearly 12 months in advance, the Secretary requires flexibility to target valuable TIP resources to address emerging needs, risks, and national priorities. Moreover, funds for this program will also allow the Department to build on and leverage partnerships with other Federal agencies and industry that seek to advance the State of the Nation's preparedness through better security solutions and information sharing approaches. Because the program is designed to provide us with maximum flexibility at the appropriate time, the Department is confident that the TIP will help further the mission of securing the homeland. The Administration requested a nearly 50 percent increase in total infrastructure funding in order to reduce concerns about "competition" among various sectors.

ALL-HAZARDS

Question. The fine men and women of FEMA have recently responded to wildfires in Alaska, mudslides in California, and hurricanes in Florida in an unprecedented period of activity. As the backbone of the nation's all-hazards emergency management system the Emergency Management Performance Grants (EMPG) Program, now administered by the Office of State and Local Government Coordination and Preparedness, is the only direct source of Federal funding to assist State and local governments with planning and preparedness activities associated with natural disasters. Congress saw fit last year to reject the President's proposal to cap allowable salary expenses and to shift the program away from its all-hazards philosophy. Secretary Chertoff said on March 2 of this year "while fighting terrorism was the reason for the department's creation, it is not our sole function," which implies that all-hazards prevention, preparedness, response and recovery is a priority of DHS.

Yet, a proposed $10 million cut in the EMPG program appeared in the Budget Request.

Why is it that the President proposes a $10 million cut in this program?

Answer. The Department's fiscal year 2006 Budget request of $170 million for the Emergency Management Performance Grants (EMPG) Program remains consistent with the fiscal year 2005 request and demonstrates a continued strong commitment and support to the nation's emergency prevention and response community through an all-hazards approach. In fiscal year 2006, EMPG will provide support for State and local emergency management departments and agencies based on identified needs and priorities for strengthening their emergency management capabilities, while addressing homeland security concerns. Further, the integration of EMPG into the Homeland Security Grant Program umbrella results in synergies with other related homeland security assistance programs. In addition, this integration also has facilitated efforts by states/local jurisdictions to leverage homeland security assistance to accomplish goals and objectives in their homeland security strategies.

FIRE GRANT FUNDING

Question. Each day firefighters put themselves in harm's way to protect property and help citizens in time of need. There are currently over 1 million active firefighters in the United States, and about 73 percent of those volunteer. According to the U.S. Fire Service, many fire departments report shortfalls in facilities, equipment, and training of personnel particularly volunteer companies in rural communities. An estimated one-third of firefighters per shift are not equipped with self-contained breathing apparatus. In communities under 10,000 in population that have at least one building 4 stories high or higher, 10 percent are estimated to have no ladder or aerial apparatus. The assessment also found that overall fire departments can only equip about half of the emergency responders on a shift with portable radios. Additionally, 21 percent of fire departments, nearly all of them predominately volunteer departments, have four or fewer firefighters available in a mid-day fire house which means it is likely that the departments fail to deliver the minimum of 4 firefighters needed to safely initiate an interior attack on a fire. Fiscally stressed communities make every effort to support public servants but State and local funding simply is not there. Yet, the President proposes to reduce firefighter grants from $715 million to $500 million. In addition, he proposes to eliminate funding for the SAFER program, which Congress authorized to help communities hire firefighters.

Please explain how the President's proposed 30 percent cut in funding helps fill these gaps.

Answer. The Department's fiscal year 2006 Budget request reflects a strong commitment to our nation's fire service by providing $500 million for the Assistance to Firefighters Grant Program. This request is consistent with the Administration's budget request since fiscal year 2003 and reflects the appropriate balance of funding priorities among DHS grant programs. Further, this program has been in existence for 5 years and has 4 years of grant experience. In its reauthorization, Congress directed that an update to an assessment of the needs of the fire service be done, as the prior assessment does not reflect the impact of more than $2 billion in grant funding that DHS has provided to the nation's fire service over the last 3 years, both through Assistance to Firefighter Grants and Homeland Security Grants. In fact, the nation's fire service has received more DHS grant funding than any other public safety discipline. This report is expected to be completed in February or March 2006. In addition, Firefighting Operations and Support for terrorist attacks, major disasters, and other emergencies is among the national target capabilities identified in the forthcoming National Preparedness Goal. Finally, it is important to note that there is significant funding available for similar purposes included in other programs, such as the State Homeland Security Program and the Urban Areas Security Initiative.

Question. Also, please explain why the President proposes to terminate the SAFER firefighter hiring program.

Answer. The Administration has requested significant funds over several years to support public safety preparedness at the State and local levels of government. Over the last 3 years, Congress has appropriated and DHS has granted over $12 billion to support training, exercising, and equipping public safety personnel, including firefighters, across the nation. The Administration maintains that hiring firefighters should remain a local responsibility, as local resources will eventually be needed to retain newly hired personnel. To that end, Federal support should focus on enhancing local capacities through training, equipment, and exercises; and not building inherently local capacities.

INTEROPERABILITY COMMUNICATIONS

Question. Over $800 million in grant funding has been distributed for interoperability projects. The next largest specific first responder category—at less than half of that—is regional response teams funding. The Intelligence Reform Act authorizes a new DHS grant program for interoperability as well as a pilot program and the ability to establish and Office of Interoperability and Compatibility.

What lessons learned or best practices has the agency gleaned from the fiscal year 2003 demonstration with COPS and FEMA?

Answer. The "fiscal year 2003 demonstration" refers to the competitive grant program that COPS, FEMA, and SAFECOM collaborated on to maximize the funding available for interoperable communications equipment. The program provided competitive funding to local jurisdictions to demonstrate effective solutions for achieving interoperability. The lessons learned from this program have been incorporated into SAFECOM's coordinated grant guidance.

SAFECOM, a program of the S&T Directorate's Office for Interoperability and Compatibility (OIC), is the umbrella program within the Federal Government that oversees all initiatives and projects pertaining to public safety communications and interoperability. SAFECOM's coordinated grant guidance provides the public safety community with consistent guidance, coordinated application processes, similar requirements across grant programs, and general guidelines for implementing a successful wireless communications system. This guidance seeks to incorporate best practices and lessons learned from the fiscal year 2003 demonstration program. The guidance was incorporated in the fiscal year 2003 FEMA and fiscal year 2003/fiscal year 2004 COPS grant awards, as well as ODP grant packages in fiscal year 2004. Examples of the lessons learned which are incorporated into the grant guidance include:

—General criteria relating to public safety communications grants;
—Criteria specific to block grants allocated to states;
—Additional criteria based on the lifecycle of public safety communications projects;
—Additional guidelines, examples, and resources for improving public safety communications and interoperability, and implementing a wireless communication system; and
—A thorough list of questions that applicants can use to help ensure that they have taken into account the needs of public safety, potential partners, and considered short and long-term goals.

SAFECOM's coordinated grant guidance is available at www.safecomprogram.gov.

Question. Outside of equipment acquisition what are the obstacles to interoperability?

Answer. While equipment acquisition is a substantial obstacle, there are many other significant challenges to achieving interoperability. In a February 2003 report, the National Task Force on Interoperability identified five key challenges facing the development of interoperability, including: limited and fragmented radio spectrum, lack of coordination and cooperation, limited and fragmented funding, incompatible and aging communications equipment, and limited and fragmented planning.

DHS understands the complexity of the problem of interoperability. The OIC, through SAFECOM—the umbrella program within the Federal Government that oversees all initiatives and projects pertaining to public safety communications and interoperability—has developed the Interoperability Continuum to serve as a framework for addressing the obstacles to interoperability, beyond just equipment. The Continuum helps the public safety community and local, tribal, state, and Federal policy makers address critical elements for success as they plan and implement interoperability solutions. These elements include governance, standard operating procedures, technology, training/exercises, and usage of interoperable communications. Making progress in each of the five critical elements is crucial to the Department providing guidance to overcome the obstacles to interoperability.

INTEROPERABILITY STANDARDS

Question. What is the status of national standards for interoperable communication?

Answer. DHS has made significant strides in the development of national standards and requirements for interoperable communications through SAFECOM. SAFECOM has developed accelerated standards for public safety interoperable communications, and drafted a report as required by IRTPA that discusses DHS plans for accelerating standards. This report includes a schedule of milestones and achievements. The report is moving through the clearance process and will be sent to Congress immediately therafter.

DHS recognizes that the development of standards can only occur within the context of an architectural framework. The SAFECOM process for identifying and developing standards begins with development of a practitioner-accepted statement of requirements which then drives the development of a Public Safety Architecture Framework (PSAF). SAFECOM released Version 1.0 of the first comprehensive Public Safety Communications and Interoperability Statement of Requirements (SoR) in 2004. Developed with public safety practitioner input, the SoR defines the functional requirements for public safety practitioners to communicate and share information when it is needed, where it is needed, and when authorized. SAFECOM, in cooperation with the National Institute of Standards Technology's (NIST) Office of Law Enforcement Standards (OLES), completed a draft of the PSAF, currently being reviewed for publication. The architectural framework outlines what the overall structured approach is for facilitating interoperability and indicates how the architecture will operate through the development of interface standards.

Since the release of v1.0 of the Public Safety Communications and Interoperability SoR, SAFECOM has undertaken the development of v1.1 of the SoR. SoR v1.1 will reorganize the requirements contained within v1.0 into a layered structure, reclassifying the requirements into Network Functional Requirements, Device Functional Requirements, and Application/Services Functional Requirements. SAFECOM is currently vetting v1.1 of the SoR with the public safety practitioner community and anticipates releasing v1.1 to the public upon completion of that vetting process.

Development of v2.0 of the SoR is currently underway. SoR v2.0 will add additional quantitative values to the functional requirements contained in v1.1, as well as address NIMS compliance. SAFECOM anticipates that it will be able to vet the draft of this version with the public safety community beginning in early 2006.

Question. What other equipment does DHS plan to publish standards for and when will those standards be published?

Answer. The Standards Portfolio in the S&T Directorate is working with voluntary consensus standards organizations and the National Institute of Standards and Technology (NIST) to develop standards in many areas of homeland security. In the CBRNE area, standards should be published in fiscal year 2005-fiscal year 2006 for: radiation detection (portal monitors, neutron detectors, training and data format); suspicious powder protocols, trace explosive detection; and chemical agent vapor detection. Standards for CBRNE personal protective equipment for emergency responders are being developed for: powered air purifying and self contained breathing respirators; chemical/biological hot and warm zone ensembles; personal alert safety systems; thermal exposure measurement; law enforcement PPE; and a bomb suit. Standards are also in development for biometric evaluation protocols, user interface guidelines, image quality. Standards efforts are in progress for: building security personal identity verification and access control; gaseous air cleaning; economic standards for security-related issues; and design/economics for structural integrity. Check lists for security of information technology products and PDA forensic tools have been published. Finally, SAFECOM is working with NIST's OLES and other Federal partners to accelerate the publishing of relevant radio standards for public safety interoperable communications in fiscal year 2006-fiscal year 2007. Standards for the Inter-Sub-System-Interface, Console Interface, and Fixed Station Interface will pave the way for future seamless communications. Standards for basic functionality will be published by the second quarter of fiscal year 2006, with the balance of the functions being published by the second quarter of fiscal year 2007.

NON-PROFIT GRANT FUNDING

Question. In fiscal year 2005, $25 million was provided for non-profits for security at high-threat facilities. Who have these awards been distributed to, for how much and for what purpose?

Answer. The $25 million was provided to protect nonprofit organizations located in the top 18 urban areas receiving funds in the fiscal year 2005 UASI program. These funds are to be used for target hardening, which includes the acquisition and installation of security equipment in real property (including buildings and improvements) owned or leased by a nonprofit organization, specifically in response to a risk of terrorist attack. Specific allocations for urban areas are available in the fiscal year 2005 Homeland Security Grant Program (HSGP) program guidelines and application kit, which can be found at the following website address: http://www.ojp.usdoj.gov/fundopps.htm

Question. Do funds remain available for obligation? If so, how much?

Answer. Upon receipt of fiscal year 2005 funds awarded through the HSGP, States were required to issue a solicitation within 60 days of the award date for or-

ganizations to apply for funds allocated for nonprofit organizations. States are currently in the process of finalizing these awards.

EMS FIRST RESPONDER FUNDING

Question. In response to a request of the Appropriations Committee, the Department recently submitted a report entitled, "Support for EMS Provided by the DHS Office of State and Local Government Coordination and Preparedness" which indicates that under the funding provided for our first responders, the Emergency Medical Services only receives about 4 percent of the total.

What information does the Department have that tells us whether 4 percent is an adequate share to prepare the professionals who will provide emergency medical care to victims at the scene of a potential attack or terrorist event?

Answer. SLGCP provides training, funds for the purchase of equipment, support for the planning and execution of exercises, technical assistance, and other support to assist states, urban areas, and local jurisdictions in preventing, planning for, and responding to acts of terrorism. SLGCP established and maintains several programs that provide these services to emergency responders, including the HSGP, the UASI, and the Assistance to Firefighters Grant Program. SLGCP grant funds can be used to enhance emergency responder capabilities, including EMS, in accordance with the goals and objectives identified in the State or urban area's homeland security strategy. Additionally, fire department-based EMS providers have been, and continue to be, eligible for assistance under the Assistance to Firefighters Grant Program.

The readiness of EMS is vital to ensuring prompt and appropriate emergency care and transportation as a component of the overall response to a terrorist incident. Therefore, it is essential that EMS agencies receive support and assistance from the States and be integrated into planning efforts and working groups to enhance the overall preparedness of state, urban area, and local public safety personnel to prevent, respond to and assist in the recovery from terrorist incidents. SLGCP funds for EMS agencies are allocated through the state's State Administrative Agencies (SAA), in accordance with each state's homeland security strategy. These strategies are based upon comprehensive assessments that address the specific vulnerabilities, threats, capabilities and needs in each state. In recognition of each state's unique threat, need, and vulnerability assessments, the Department does not dictate a specific percentage of funds that should be allocated to supplant EMS services. Instead, the Department supports a distribution strategy capable of addressing the distinctive needs of EMS agencies by allowing specific allocation amounts to be determined at the discretion of each state. However, in recognition of the important role played by EMS providers, the Department issued an Information Bulletin on May 6, 2004. The Information Bulletin reminded States that EMS providers are eligible to receive funding under the State HSGP and UASI programs.

PORT SECURITY GRANT COORDINATION

Question. What coordination is occurring among states, local port authorities and the Captains of the Port, to ensure all vested parties are aware of grant determinations and that the limited resources are maximized when port security grants are made to independent terminal operators?

Answer. As part of the transition of the Port Security Grant (PSG) Program from TSA to SLGCP, the Department has completely redesigned the process to focus on the risk-based prioritization of ports and allocation of the funds to address specific national port security priorities from a port-wide perspective. Redesign of the program was a collaborative process between SLGCP, the U.S. Coast Guard (USCG), the Information Analysis and Infrastructure Protection Directorate (IAIP), the Maritime Administration (MARAD) within DOT, and the American Association of Port Authorities (AAPA), among others. As part of this process the USCG Captain of the Port (COTP) will coordinate a field review of all projects submitted for funding consideration. This field review will be conducted in coordination with the MARAD Region Director, the SAA responsible for the state's Homeland Security Strategy, and appropriate members of each port area's Area Maritime Security Committee (which includes representatives of the local port authorities) to ensure that a port-wide approach to risk reduction is taken and that scarce resources are maximized. Lastly, when determinations of funding have been made, a consolidated list of projects for each port area will be provided to the COTP, MARAD Region Director, SAA, and relevant members of the Area Maritime Security Committee.

TECHNOLOGY TRANSFER

Question. How much of the $50 million appropriated for the Technology Transfer Program has been awarded, to whom and for what projects?

Answer. The Technology Transfer Program is known as the Commercial Equipment Direct Assistance Program (CEDAP). The legislation set aside $10 million for testing and evaluation of commercially available equipment to determine appropriateness for inclusion in the CEDAP program. The remaining $40 million was dedicated to the CEDAP program.

On March 22, 2005, SLGCP officially opened the CEDAP to applications. The applications are competitive and must be consistent with the State homeland security plan. This first pilot test of the program ended May 5, 2005, with applications from 1,500 agencies for $34.4 million in equipment. The first award to 214 agencies of $2.0 million in equipment and training will take place June 15, 2005. (See table below.)

Phase II of the CEDAP program will begin with the opening of the application process in the summer of 2005. Award of the equipment and hands on training for the accepted applicants will take place early in the fall of 2005.

CEDAP AWARDS, ROUND #1—AGENCY BY STATE

[Total Agencies: 214]

State/Agency	City	Technology	Type	Unit Cost
Alabama:				
Alexander City Fire Department	Alexander City	Thermal Imager	Fire Department	$12,500.00
Atmore Police Department	Atmore	Search Camera Victim Locator System	Law Enforcement	14,620.00
Brick Hatton Volunteer Fire Department	Town Creek	Thermal Imager	Fire Department	12,500.00
Calera Fire Department	Calera	Thermal Imager	Fire Department	12,500.00
Calera Police Department	Calera	Search Camera Victim Locator System	Law Enforcement	14,620.00
Cherokee Rescue Squad	Cherokee	Search Camera Victim Locator System	Emergency Medical Services	14,620.00
Cherokee Volunteer Fire Fighters	Cherokee	Thermal Imager	Fire Department	12,500.00
Choctaw County Emergency Management Agency	Butler	Thermal Imager	Emergency Management	12,500.00
Cottonwood Police Department	Cottonwood	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Daphne Police Department	Daphne	Night Vision Kit	Law Enforcement	3,700.00
Georgiana Police Department	Georgiana	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Guntersville Fire/Rescue	Guntersville	Thermal Imager	Fire Department	12,500.00
Jasper Police Department	Jasper	Thermal Imager	Law Enforcement	12,500.00
Margaret Fire and Rescue	Margaret	Thermal Imager	Fire Department	12,500.00
Phoenix City Police Department	Phoenix City	Night Vision Kit	Law Enforcement	3,700.00
Russell County Sheriff's Department	Phoenix City	Night Vision Kit	Public Safety	3,700.00
Alaska:				
Kodiak Police Department	Kodiak	Night Vision Kit	Law Enforcement	3,700.00
Arizona:				
Safford Police Department	Safford	Search Camera Victim Locator System	Law Enforcement	14,620.00
Arkansas:				
Clinton Police Department	Clinton	Thermal Imager	Law Enforcement	12,500.00
Ouachita County Sheriff's Department	Camden	Night Vision Kit	Law Enforcement	3,700.00
Sherwood Police Department	Sherwood	Search Camera Victim Locator System	Law Enforcement	14,620.00
California:				
Greenfield Police Department	Greenfield	Thermal Imager	Law Enforcement	12,500.00
Humboldt County Sheriff's Office	Eureka	Thermal Imager	Law Enforcement	12,500.00
Mariposa County Sheriff's Office	Mariposa	Night Vision Kit	Law Enforcement	3,700.00
Monterey Peninsula Airport Police	Monterey	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
San Rafael Police Department	San Rafael	Thermal Imager	Law Enforcement	12,500.00
Colorado:				
Idaho Springs Police Department	Idaho Springs	Night Vision Kit	Law Enforcement	3,700.00
Manitou Springs Police Department	Manitou Springs	Thermal Imager	Law Enforcement	12,500.00

CEDAP AWARDS, ROUND #1—AGENCY BY STATE—Continued

[Total Agencies: 214]

State/Agency	City	Technology	Type	Unit Cost
Connecticut:				
Mohegan Tribal Fire Department	Uncasville	Night Vision Kit	Public Safety	3,700.00
Putnam Police Department	Putnam	Thermal Imager	Law Enforcement	12,500.00
Torrington Police Department	Torrington	Night Vision Kit	Law Enforcement	3,700.00
Town of Stafford	Stafford	Night Vision Kit	Law Enforcement	3,700.00
Delaware:				
Elsmere Bureau of Police	Elsmere	Thermal Imager	Fire Department	12,500.00
New Castle Police Department	New Castle	Thermal Imager	Law Enforcement	12,500.00
Florida:				
Florida Gulf Coast University Police	Fort Myers	Thermal Imager	Law Enforcement	12,500.00
Havana Police Department	Havana	Thermal Imager	Law Enforcement	12,500.00
Kissimmee Police Department	Kissimmee	Thermal Imager	Law Enforcement	12,500.00
Winter Springs Police Department	Winter Springs	Thermal Imager	Law Enforcement	12,500.00
Georgia:				
Austell Police Department	Austell	Night Vision Kit	Law Enforcement	3,700.00
Jackson County Sheriff's Office	Jefferson	Thermal Imager	Law Enforcement	12,500.00
Idaho:				
Madison County Sheriff's Office	Rexburg	Thermal Imager	Law Enforcement	12,500.00
Rexburg Police Department	Rexburg	Thermal Imager	Law Enforcement	12,500.00
Illinois:				
Elkville Volunteer Fire Department	Dowell	Thermal Imager	Fire Department	12,500.00
Homewood Police Department	Homewood	Thermal Imager	Law Enforcement	12,500.00
Olney Fire Department	Olney	Thermal Imager	Fire Department	12,500.00
Indiana:				
Francesville Volunteer Fire Department	Francesville	Thermal Imager	Fire Department	12,500.00
Hudson Marshal's Office	Hudson	Night Vision Kit	Law Enforcement	3,700.00
Wayne County Sheriff's Office	Richmond	Thermal Imager	Law Enforcement	12,500.00
Iowa:				
Cedar Falls Police Department	Cedar Falls	Search Camera Victim Locator System	Law Enforcement	14,620.00
Eldridge Volunteer Fire Company, Inc.	Eldridge	CEDAP Personal Protective Equipment Kit	Fire Department	4,140.00
Marion County Sheriff's Office	Knoxville	Night Vision Kit	Law Enforcement	3,700.00
Poweshiek County Emergency Management Agency	Grinnell	CEDAP Personal Protective Equipment Kit	HAZMAT	4,140.00
Scott County Sheriff's Office	Davenport	Thermal Imager	Public Safety	12,500.00
Sheldon Police Department	Sheldon	Thermal Imager	Law Enforcement	12,500.00

Kansas:				
Rose Hill Police Department	Rose Hill	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Washington County Sheriff's Department	Washington	Night Vision Kit	Law Enforcement	3,700.00
Kentucky:				
Bourbon County Sheriff's Office	Paris	Thermal Imager	Fire Department	12,500.00
Louisiana:				
District 8 Fire Department	Rayville	Thermal Imager	Fire Department	12,500.00
Grant Parish Sheriff's Office	Colfax	Search Camera Victim Locator System	Law Enforcement	14,620.00
Jackson Parish Sheriff's Department	Jonesboro	Night Vision Kit	Law Enforcement	3,700.00
Lincoln Parish Sheriff's Department	Ruston	Night Vision Kit	Law Enforcement	3,700.00
Richland Parish Sheriff's Office	Rayville	Night Vision Kit	Law Enforcement	3,700.00
Rosepine Police Department	Rosepine	Night Vision Kit	Law Enforcement	3,700.00
St. James Parish Sheriff's Office	Vacherie	Search Camera Victim Locator System	Law Enforcement	14,620.00
West Monroe Police Department	West Monroe	Night Vision Kit	Law Enforcement	3,700.00
Maine:				
Ashland Police Department	Ashland	Night Vision Kit	Law Enforcement	3,700.00
Westbrook Fire Rescue Department	Westbrook	Search Camera Victim Locator System	Fire Department	14,620.00
Massachusetts:				
Burlington Police Department	Burlington	Night Vision Kit	Law Enforcement	3,700.00
Fairhaven Police Department	Fairhaven	Night Vision Kit	Law Enforcement	3,700.00
Gardner Police Department	Gardner	Night Vision Kit	Law Enforcement	3,700.00
Granby Police Department	Granby	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Nantucket Fire Department	Nantucket	Thermal Imager	Fire Department	12,500.00
Norwood Fire Department	Norwood	Thermal Imager	Fire Department	12,500.00
Plymouth Police Department	Plymouth	Thermal Imager	Law Enforcement	12,500.00
Saugus Emergency Management Agency	Saugus	Thermal Imager	Emergency Management	12,500.00
Wayland Police Department	Wayland	Thermal Imager	Law Enforcement	12,500.00
Michigan:				
Gogebic County Emergency Management	Bessemer	Thermal Imager	Emergency Management	12,500.00
Grosse Ile Police Department	Grosse Ile	Thermal Imager	Law Enforcement	12,500.00
Hampton Township Fire Department	Essexville	Thermal Imager	Fire Department	12,500.00
Harper Woods Police Department	Harper Woods	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Kent County Sheriff's Department	Grand Rapids	Night Vision Kit	Law Enforcement	3,700.00
Minnesota:				
Annandale Fire Department	Annandale	Thermal Imager	Fire Department	12,500.00
Cleveland Police Department	Cleveland	Thermal Imager	Law Enforcement	12,500.00
Douglas County Sheriff's Office	Alexandria	Thermal Imager	Law Enforcement	12,500.00
Elk River Police Department	Elk River	Thermal Imager	Law Enforcement	12,500.00
Hector Police Department	Hector	Night Vision Kit	Law Enforcement	3,700.00
Mentor Volunteer Fire and Rescue	Mentor	Night Vision Kit	Fire Department	3,700.00

CEDAP AWARDS, ROUND #1—AGENCY BY STATE—Continued

[Total Agencies: 214]

State/Agency	City	Technology	Type	Unit Cost
Nicollet County Sheriff's Office	St. Peter	Search Camera Victim Locator System	Law Enforcement	14,620.00
Red Lake County Sheriff's Office/OEM	Red Lake Falls	Night Vision Kit	Law Enforcement	3,700.00
Winona County Sheriff's Department	Winona	Thermal Imager	Law Enforcement	12,500.00
Winona Police Department	Winona	Search Camera Victim Locator System	Law Enforcement	14,620.00
Mississippi:				
Clarkdale Fire & Rescue	Meridian	Search Camera Victim Locator System	Fire Department	14,620.00
North Haven Volunteer Fire Department	New Albany	Thermal Imager	Fire Department	12,500.00
Tippah County Sheriff's Department	Ripley	Thermal Imager	Law Enforcement	12,500.00
Missouri:				
Buchanan County Sheriff's Office	St. Joseph	Thermal Imager	Law Enforcement	12,500.00
JasCo Metropolitan Police Department	Oronogo	Night Vision Kit	Law Enforcement	3,700.00
Jonesburg Police Department	Jonesburg	Advanced Portable Detector	Law Enforcement	10,200.00
Kelso Police Department	Kelso	Search Camera Victim Locator System	Law Enforcement	14,620.00
Madison County Sheriff's Department	Fredericktown	Thermal Imager	Law Enforcement	12,500.00
Park Hills Police Department	Park Hills	Thermal Imager	Law Enforcement	12,500.00
Sni Valley Fire Protection District	Oak Grove	Thermal Imager	Fire Department	12,500.00
Terre du Lac Fire and Rescue	Bonne Terre	Thermal Imager	Fire Department	12,500.00
Nebraska:				
Cuming County Sheriff's Office	West Point	Thermal Imager	Law Enforcement	12,500.00
Grand Island Police Department	Grand Island	Night Vision Kit	Law Enforcement	3,700.00
Hall County Sheriff's Department	Grand Island	Thermal Imager	Law Enforcement	12,500.00
Hay Springs Police Department	Hay Springs	Night Vision Kit	Law Enforcement	3,700.00
Keith County Sheriff's Department	Ogallala	Thermal Imager	Law Enforcement	12,500.00
Platte County Sheriff's Department	Columbus	Thermal Imager	Law Enforcement	12,500.00
Wayne County Sheriff's Office	Wayne	Night Vision Kit	Law Enforcement	3,700.00
New Hampshire:				
Allenstown Police Department	Allenstown	Night Vision Kit	Law Enforcement	3,700.00
Durham Police Department	Durham	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
New Jersey:				
Cinnaminson Township Police Department	Cinnaminson	Night Vision Kit	Law Enforcement	3,700.00
Clark Police Department	Clark	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Franklin Township Police Department	Pittstown	Night Vision Kit	Law Enforcement	3,700.00
Glen Ridge Police Department	Glen Ridge	Night Vision Kit	Law Enforcement	3,700.00
Magnolia Police Department	Magnolia	Thermal Imager	Law Enforcement	12,500.00
Ridgefield Police Department	Ridgefield	Thermal Imager	Law Enforcement	12,500.00

Sea Girt Borough Police and Fire Departments	Sea Girt	Advanced Portable Detector	Other	10,200.00
Washington Township Police Department	Robbinsville	Thermal Imager	Law Enforcement	12,500.00
Waterford Township Fire Department	Atco	Thermal Imager	Fire Department	12,500.00
Waterford Township Police Department	Atco	Night Vision Kit	Law Enforcement	3,700.00
New York:				
Harriman Police Department	Harriman	Night Vision Kit	Law Enforcement	3,700.00
Melrose Fire District	Melrose	Thermal Imager	Fire Department	12,500.00
New Windsor Police Department	New Windsor	Thermal Imager	Law Enforcement	12,500.00
North Carolina:				
Beaufort Police Department	Beaufort	Thermal Imager	Law Enforcement	12,500.00
Forest City Fire Department	Forest City	Thermal Imager	Fire Department	12,500.00
McDowell County Emergency Management	Marion	Thermal Imager	Emergency Management	12,500.00
Rocky Mount Police Department	Rocky Mount	Night Vision Kit	Law Enforcement	3,700.00
Rutherfordton Fire Department	Rutherfordton	Thermal Imager	Fire Department	12,500.00
Trent Woods Police Department	Trent Woods	Night Vision Kit	Law Enforcement	3,700.00
North Dakota:				
New England Fire Department	New England	Thermal Imager	Fire Department	12,500.00
Stark County Sheriff's Department	Dickinson	Thermal Imager	Law Enforcement	12,500.00
Ohio:				
Akron Police Department	Akron	Night Vision Kit	Law Enforcement	3,700.00
Beavercreek Police Department	Beavercreek	Night Vision Kit	Law Enforcement	3,700.00
Northwest Ambulance District	Geneva	Advanced Portable Detector	Emergency Medical Services	10,200.00
Oklahoma:				
Enid Fire Department	Enid	Thermal Imager	Fire Department	12,500.00
Marlow Police Department	Marlow	Thermal Imager	Law Enforcement	12,500.00
Owasso Fire Department	Owasso	Thermal Imager	Fire Department	12,500.00
Woodward Police Department	Woodward	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Oregon:				
Cascade Locks Fire & Emergency Medical Services	Cascade Locks	Thermal Imager	Other	12,500.00
Hubbard Police Department	Hubbard	Night Vision Kit	Law Enforcement	3,700.00
Illinois Valley Fire District	Cave Junction	Thermal Imager	Fire Department	12,500.00
Malheur County Sheriff's Office	Vale	Thermal Imager	Law Enforcement	12,500.00
Oakland Rural Fire District	Oakland	Thermal Imager	Fire Department	12,500.00
Turner Police Department	Turner	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Turner Rural Fire Protection District	Turner	Thermal Imager	Fire Department	12,500.00
Pennsylvania:				
Bristol Township Police Department	Bristol	Thermal Imager	Law Enforcement	12,500.00
Millersville Borough Police Department	Millersville	Night Vision Kit	Law Enforcement	3,700.00
Wilkes-Barre Police Department	Wilkes-Barre	Thermal Imager	Law Enforcement	12,500.00
Wilkes-Barre Township Police Department	Wilkes-Barre	Thermal Imager	Law Enforcement	12,500.00

CEDAP AWARDS, ROUND #1—AGENCY BY STATE—Continued

[Total Agencies: 214]

State/Agency	City	Technology	Type	Unit Cost
Rhode Island:				
Bristol Police Department	Bristol	Thermal Imager	Law Enforcement	12,500.00
Cumberland Hill Fire District	Cumberland	Thermal Imager	Fire Department	12,500.00
North Smithfield Fire & Rescue Service	North Smithfield	Thermal Imager	Fire Department	12,500.00
Pawtucket Fire Department	Pawtucket	Thermal Imager	Fire Department	12,500.00
South Carolina:				
Hardeeville Fire/Rescue	Hardeeville	Thermal Imager	Fire Department	12,500.00
Tennessee:				
Lenoir City Police Department	Lenoir City	Night Vision Kit	Law Enforcement	3,700.00
Martin Fire Department	Martin	Thermal Imager	Fire Department	12,500.00
Milan Police Department	Milan	Night Vision Kit	Law Enforcement	3,700.00
Texas:				
Arp Marshal's Office	Arp	Thermal Imager	Emergency Management	12,500.00
Bosque County Constable's Office—Precinct 1	Meridian	Night Vision Kit	Law Enforcement	3,700.00
Brownsboro Police Department	Brownsboro	Thermal Imager	Law Enforcement	12,500.00
Clifton Volunteer Fire Department	Clifton	Search Camera Victim Locator System	Fire Department	14,620.00
Cockrell Hill Police Department	Dallas	Night Vision Kit	Law Enforcement	3,700.00
Conroe Fire Department	Conroe	Thermal Imager	Fire Department	12,500.00
Crims Chapel Volunteer Fire Department	Henderson	Thermal Imager	Fire Department	12,500.00
Gainesville Police Department	Gainesville	Night Vision Kit	Law Enforcement	3,700.00
Hillsboro Fire/Rescue	Hillsboro	Thermal Imager	Fire Department	12,500.00
Jacksboro Police Department	Jacksboro	Thermal Imager	Law Enforcement	12,500.00
Marietta Volunteer Fire Department	Marietta	Thermal Imager	Fire Department	12,500.00
Meridian Fire Department	Meridian	Thermal Imager	Fire Department	12,500.00
Valley Mills Police Department	Valley Mills	Thermal Imager	Law Enforcement	12,500.00
Victoria Police Department	Victoria	Advanced Portable Detector	Law Enforcement	10,200.00
Wichita County Texas Emergency Management	Wichita Falls	Search Camera Victim Locator System	Emergency Management	14,620.00
Winters Police Department	Winters	Night Vision Kit	Law Enforcement	3,700.00
Utah:				
Cedar City/Iron County Fire Department	Cedar City	Thermal Imager	Fire Department	12,500.00
Emery County Sheriff's Office	Castle Dale	Night Vision Kit	Law Enforcement	3,700.00
Helper Police Department	Helper	Thermal Imager	Law Enforcement	12,500.00
Morgan County Sheriff's Office	Morgan	Thermal Imager	Law Enforcement	12,500.00
Virginia:				
Amherst County Sheriff's Office	Amherst	Thermal Imager	Law Enforcement	12,500.00

Buena Vista Police Department	Buena Vista	Night Vision Kit	Public Safety	3,700.00
Cumberland County Sheriff's Office	Cumberland	Thermal Imager	Law Enforcement	12,500.00
Emporia Police Department	Emporia	Search Camera Victim Locator System	Law Enforcement	14,620.00
Henry County Sheriff's Office	Martinsville	Night Vision Kit	Law Enforcement	3,700.00
King George Sheriff's Office	King George	Thermal Imager	Law Enforcement	12,500.00
Washington:				
Bainbridge Island Police Department	Bainbridge Island	Thermal Imager	Law Enforcement	12,500.00
Chelan County Sheriff's Office	Wenatchee	Thermal Imager	Law Enforcement	12,500.00
Columbia County Sheriff's Office	Dayton	Night Vision Kit	Law Enforcement	3,700.00
Colville Police Department	Colville	Thermal Imager	Law Enforcement	12,500.00
Colville Tribes Fire Rescue	Nespelem	Thermal Imager	Fire Department	12,500.00
Jefferson County Sheriff's Office	Port Hadlock	Thermal Imager	Law Enforcement	12,500.00
Kettle Falls Police Department	Kettle Falls	Night Vision Kit	Law Enforcement	3,700.00
Lakewood Police Department	Lakewood	Search Camera Victim Locator System	Law Enforcement	14,620.00
Pierce County Fire District 18	Orting	Thermal Imager	Fire Department	12,500.00
San Juan County Sheriff's Office	Eastsound	Night Vision Kit	Fire Department	3,700.00
San Juan Fire District 3	Friday Harbor	Thermal Imager	Law Enforcement	12,500.00
Stevens County Fire District 2	Hunters	Thermal Imager	Fire Department	12,500.00
Stevens County Fire Protection District 1	Clayton	Thermal Imager	Fire Department	12,500.00
Stevens County Sheriff's Ambulance	Colville	Night Vision Kit	Emergency Medical Services	3,700.00
Sumas Police Department	Sumas	Thermal Imager	Law Enforcement	12,500.00
Tumwater Police Department	Tumwater	Night Vision Kit	Law Enforcement	3,700.00
Walla Walla Police Department	Walla Walla	Search Camera Victim Locator System	Law Enforcement	14,620.00
Wisconsin:				
Auburndale Joint Fire and Rescue Department	Auburndale	Thermal Imager	Fire Department	12,500.00
Chippewa Falls Fire and Emergency Services	Chippewa Falls	Thermal Imager	Fire Department	12,500.00
Chippewa Falls Police Department	Chippewa Falls	Night Vision Kit	Law Enforcement	3,700.00
Chippewa Fire District	Chippewa Falls	Thermal Imager	Fire Department	12,500.00
Cottage Grove Police Department	Cottage Grove	Night Vision Kit	Law Enforcement	3,700.00
Fox Valley Metro Police Department	Little Chute	Night Vision Kit	Law Enforcement	3,700.00
Germantown Police Department	Germantown	Night Vision Kit	Law Enforcement	3,700.00
McFarland Police Department	McFarland	Night Vision Kit	Law Enforcement	3,700.00
Mishicot Police Department	Mishicot	Search Camera Victim Locator System	Law Enforcement	14,620.00
Park Falls Police Department	Park Falls	Night Vision Kit	Law Enforcement	3,700.00
Sharon Police Department	Sharon	Thermal Imager	Law Enforcement	12,500.00
Stanley Fire Department	Stanley	Search Camera Victim Locator System	Fire Department	14,620.00
Vernon County Emergency Management	Viroqua	Night Vision Kit	Law Enforcement	3,700.00

Question. What success have come out of the technology transfer program?

Answer. The first award to 214 agencies of $2.0 million in equipment and training took place on May 19, 2005. The second award will take place in the coming weeks. A detailed evaluation is under development to determine the impact and cost effectiveness of the CEDAP program.

CITIZENS CORP

Question. For what, specifically, will the increase of $35 million for Citizens Corp in the fiscal year 2006 President's Request be used?

Answer. The Citizen Corps Program (CCP) is the Department's grass-roots initiative to actively involve all citizens in hometown security through personal preparedness, training, and volunteer service. CCP funds support Citizen Corps Councils with efforts to engage citizens in preventing, preparing for, and responding to all hazards, including planning and evaluation, public education and communication, training, participation in exercises, providing proper equipment to citizens with a role in response, and management of Citizen Corps volunteer programs and activities. State and local governments have embraced the concept of Citizen Corps. They are developing the management capacity of the Councils, conducting public education, providing training for citizens, and engaging citizens through volunteer programs. However, there is a need to expand this effort to ensure that citizens are integrated in all aspects of State and local government preparedness, response and recovery and to support more significant community outreach through schools, private and public sector worksites, faith-based organizations, recreational outlets, and local media. The requested $50 million is critical to meet the demand and build the capacity of preparing, training, and involving citizens. In the end, this will result in the development of a fully-prepared community, with citizens who are fully aware, trained and practiced on how to detect, deter, prepare for, and respond to all hazards and threats.

BEST PRACTICES

Question. As the Office of State and Local Government Coordination and Preparedness discovers lessons learned and best practices across the Nation regarding procurement and allocation of grant funding, are those practices being collected and made available for State and local governments to benefit?

Answer. SLGCP currently has several avenues to identify and share grant-related best practices and lessons learned with its State and local grantees.

—The office has analyzed the states' and territories' narrative on management capabilities responses included in the fiscal year 2005 HSGP applications, including information on allocation of grant funding. SLGCP will provide each respondent with a written overview summary analysis that highlights best management practices and lessons learned. This overview will allow States to learn about approaches that are working successfully in other states. In addition to the overview, SLGCP will also provide a state-specific analysis of the management capabilities outlined in the applications.

—SLGCP is developing a Program Management Handbook that includes guidelines for building strong program management infrastructures. These guidelines have been written to provide a common, flexible framework with potential for customization at the state, regional, and local levels. Best practices in program management will be collected and disseminated to support the implementation of the capabilities outlined in the Handbook.

—ODP is exploring ways to provide procurement assistance including identification and dissemination of procurement best practices to help States develop streamlined procurement practices. Currently under development is procurement technical assistance including informational materials, tools and templates, and customized on-site guidance.

AIRBORNE RAPID IMAGING FOR EMERGENCY SUPPORT

Question. In the aftermath of the September 11 terrorist attacks on the World Trade Center, the State of New York utilized a technology that provided maps to first responders showing location, elevation, and temperature ranges of features on the ground within 8–10 hours after data collection. The Department of Homeland Security's Office of State and local Government Coordination and Preparedness provided $3 million in 2004 to demonstrate and further improve this technology by reducing turn around time through a system called the Airborne Rapid Imaging for Emergency Support (ARIES).

What were the results of the ARIES flight demonstration that was conducted last November?

Answer. The Airborne Rapid Imaging for Emergency Support (ARIES) program was a DHS-funded initiative to explore the technical feasibility of providing near real-time map-quality imagery for first responders in the event of a crisis. The program began in the spring of 2004 and culminated with a technical demonstration on November 17, 2004 at Picatinny Arsenal in New Jersey. The objectives of the demonstration were as follows:

—Demonstrate the capacity to obtain digital imagery rapidly using commercial aircraft in a simulated emergency event.
—Downlink this imagery directly from the aircraft to a receiving station using micro millimeter wave technology.
—Process the raw, uncorrected imagery in a portable environment for use by existing DHS systems within 3 hours of acquisition.
—Distribute the imagery to multiple agencies for emergency needs.
—Provide on-site visualization, tracking, and information gathering capabilities to assist with any emergency response requirements.

The demonstration satisfied the technical criteria for four of the five components. Distribution of the imagery was not successfully demonstrated. This was a technical demonstration that did not address the utility of ARIES' orthorectified imagery products to emergency responders.

Overall, the ARIES program proved the technical feasibility of the concept. A final program report including a costing analysis of the ARIES concept was conducted by the Institute for Defense Analysis. The report is in the final review process and will be made available upon completion.

Question. What is the current capability in Federal, state, or local government organizations or private industry to provide integrated digital imagery, lidar, and thermal information to first responders?

Answer. Many types of imagery, acquired for particular uses, are available commercially to support first responders. The capability of various organizations to deliver this imagery directly to first responders varies significantly from State to state. However, the capability of first responders to receive it and do sophisticated analysis is limited because there is no end-to-end system in place to acquire process and deliver imaging products to the first response community. The DHS Geospatial Management Office (GMO) is currently conducting pilot programs to demonstrate delivery of geospatial products to first responders using wireless hand held devices.

Question. What is the Department's need and plan to advance and utilize this technology?

Answer. According to the DHS GMO, the simultaneous collection, processing and integration of Digital Electro-optical (EO) Imagery, Light Detection and Ranging (LIDAR) elevation data and Thermal Infrared (TIR) Imagery from a single aerial platform was demonstrated in the ARIES pilot. The ARIES demonstration provided a unique capability determined to be necessary in the aftermath of September 11. Imaging technologies are collected and used by Federal, State or local organizations in a variety of mapping applications or special studies. Currently, however, the acquisition, dissemination and use of airborne and space-borne sensor information for emergency response are mostly uncoordinated among levels of government, across jurisdictions and between mission areas.

The DHS GMO is responsible for providing leadership and coordination in meeting the geospatial information requirements of those responsible for planning, prevention, mitigation, assessment and response to emergencies, critical infrastructure protection, and other functions of the Department. The GMO is working with the DHS components as well as other Federal, State and local organizations to understand the geospatial information needed to support their missions. The GMO developed the Geospatial User Needs Assessment Report which identified many of the needs. The GMO has also produced and is maintaining the Geospatial View of the Geospatial Enterprise Architecture which is a current view of the as-is and target geospatial information technology architecture for DHS. The DHS Geospatial Architecture view is referenced in the fiscal year 2005 HSGP and is being used as a model for the emerging Geospatial Profile. As the DHS and HLS architecture mature, rapid geospatial imagery acquisition requirements will be identified and services will be acquired.

HAZARD MITIGATION

Question. The Hazard Mitigation Grant Program provides critical funding to States following a declared natural disaster to assist them in reducing future disaster losses. The funding is an amount equivalent to a percentage of eligible FEMA funds. The funds provided are 75 percent Federal and 25 percent local or State. Since the passage in December 2000 of the Disaster Mitigation Act which amended

the Stafford Disaster Relief Act, FEMA has encouraged States to put forth the additional effort required to obtain an approved enhanced plan. Those with an enhanced plan would be eligible for an amount equivalent to up to 20 percent of eligible FEMA funds. Based on this incentive numerous States are working to obtain this goal. The fiscal year 2006 President's Budget proposes language to reduce the percentage to up to 12.5 percent.

Since this incentive has been in the law for 4 years, why are you requesting this change now that some States have put forth significant commitment of already overburdened resources to achieve enhanced status?

Answer. The President's Budget request preserves the 5 percent incentive for developing enhanced mitigation plans. The Hazard Mitigation Grant Program (HMGP) now uses a 7.5-percent multiplier to calculate the amount of mitigation money available to a State after a disaster declaration, when the State has an approved basic mitigation plan. When the State has an approved enhanced mitigation plan, it is eligible for up to 12.5 percent. Both the Administration and Congress agreed to the 7.5 percent basic formula, which was changed from 15 percent when Congress created the Pre-disaster Mitigation (PDM) program to provide additional funding for mitigation activities on a nationally competitive basis.

The incentive was 5 percent when the program used a 15 percent baseline and when HMGP represented the primary means for States to receive Federal mitigation funds. The incentive remains 5 percent now. Under the old plan, only the States in which a disaster was declared were eligible. However, the availability of PDM grant funds allows the States to compete for mitigation funds without a Presidential disaster declaration. The budget request of up to 12.5 percent HMGP for the States with enhanced mitigation plans preserves the 5 percentage point incentive authorized in the Disaster Mitigation Act of 2000.

Question. Which States have approved plans and which States are in the process of working on enhanced plans?

Answer. All 50 States now have approved State Mitigation Plans. In addition, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, American Samoa, Guam, the Commonwealth of the Northern Mariana Islands, and the Republic of the Marshall Islands have approved state-level mitigation plans. (The Federated States of Micronesia is the only non-Tribal jurisdiction without an approved plan. FEMA Region IX expects to be able to approve it soon.)

There are currently four States with approved enhanced mitigation plans: Missouri, Ohio, Oklahoma, and Washington. FEMA has recently reviewed enhanced plans from Maryland and Pennsylvania; however, they require revision prior to approval. The following States have advised FEMA that they may submit enhanced plans for review and approval within the next 6 months: Alabama, Florida, Georgia, Iowa, Louisiana, Minnesota, Mississippi, North Carolina, Oregon, Texas, Virginia, and Wisconsin. Arizona, California, Delaware, North Dakota, and Utah have expressed interest in developing enhanced mitigation plans, but, to date, such plans have not been received.

Question. Were the States advised that you intended to reduce the incentive?

Answer. The fiscal year 2006 President's Budget is the first time that a specific percentage, other than 20 percent, has been communicated to the States working on enhanced plans. The incentive for an enhanced plan, however, remains 5 percent.

FLOOD MAP MODERNIZATION

Question. What is the schedule, by state, for implementation of the Flood Map Modernization Program?

Answer. The schedule varies from State to State and changes from year to year. FEMA has developed a strong business planning process in which it works with the States and with other significant mapping partners to identify and schedule mapping projects jointly. FEMA then works with its partners to execute the plan based on the funding appropriated and makes adjustments twice a year to align schedules with current realities. FEMA balances stakeholder input with national and regional flood mapping needs to develop a nationwide plan for flood map update schedules and anticipated budgets. FEMA used stakeholder input to develop the initial plan, and received additional feedback on the plan that will be addressed in future updates. The current Multi-year Flood Hazard Identification Plan (MHIP), detailing the 5 year schedule and budget for developing the updated flood hazard data and maps, can be accessed online at http://www.fema.gov/fhm/mh_main.shtm.

Question. Are we on track to complete this project within the projected timeframe of completion in fiscal year 2008 within the budget that has been appropriated and requested?

Answer. FEMA is on track to complete the project by 2010, should the funding requested through 2008 be provided. That is, studies funded in 2008 are expected to be complete by 2010. The digital flood hazard data will meet quality standards contained in the MHIP. However, stakeholders have identified additional engineering requirements beyond what can be accomplished within this project. Data on these additional engineering requirements are being collected as FEMA coordinates with States and communities during the nationwide mapping effort. These data will provide the basis for evaluating future resource needs.

Question. What sort of cooperation is happening with State and local governments?

Answer. The map modernization effort is built upon constant collaboration between FEMA Headquarters and FEMA Regions I–X, the States and local entities, and the business planning process facilitates this collaboration. Many FEMA mapping partners are contributing not only to the flood map production process, but to the planning process as well. In fiscal year 2003 and fiscal year 2004, FEMA provided more than $92 million directly to its Cooperating Technical Partners (CTPs) to develop flood map data in support of map modernization. Also, in 2002, as part of its broader effort to incorporate local, state, and regional involvement in flood mapping, FEMA asked the states, territories, and some CTPs with multi-jurisdictional responsibility for floodplain management to prepare map modernization plans. The plans included extensive flood mapping needs assessments that were developed pursuant to FEMA and other criteria. In early fiscal year 2004, FEMA made funds available through the Flood Map Modernization Management Support (FMMMS) program to these same entities to upgrade and update their plans. FEMA received a total of 55 plans covering 48 States and four of the five water management districts in Florida. FEMA also received plans from the District of Columbia and two Territories.

The FMMMS program, with more than 50 partners, provides a means to ensure that partners can support Flood Map Modernization through administration and management activities. These activities, although not directly resulting in the production of a flood map, increase partners' investment and capability to manage their flood hazard data, strongly bolster the efforts of mapping partners, and ensure a tailored, local focus within a national program. Two of the most vital outcomes of FMMMS are the partners' ability to review program planning policy and guidance and their identification of needs as a part of their business planning process.

Question. What will the maintenance cost of this program be once the modernization piece is completed?

Answer. FEMA is currently estimating maintenance costs and will provide this information to the Office of Management and Budget as scheduled. The strong partnerships, business planning processes, and flood mapping technologies deployed as part of Flood Map Modernization will allow FEMA to improve its estimated maintenance costs as the program draws to completion. FEMA will continue to work with the States and communities to define the most efficient and effective approach for providing and maintaining up-to-date flood hazard information for the nation.

CERRO GRANDE FIRE CLAIMS

Question. What is the unobligated balance of the Cerro Grande fire claims fund?

Answer. As of April 30, 2005, the unobligated balance of the Cerro Grande fire claims fund is $36,559,305.

Question. Is there a deadline for claims? If so, what is it?

Answer. The deadline for filing claims (other than mitigation claims) with the Office of Cerro Grande Fire Claims was August 28, 2002. The deadline for filing mitigation claims was August 28, 2003.

Question. If it has passed, what is the remaining balance of the fund?

Answer. As of April 30, 2005, the remaining unobligated balance of the Cerro Grande fire claims fund is $36,559,305.

Question. How many claims totaling how much are left to be resolved and what is the timeline for resolving those claims?

Answer. FEMA has successfully processed 21,453 claims, including all administrative appeals. There are two claims left to be resolved. Those claims, totaling $5,249,866, were filed in the United States District Court for New Mexico. The resolution of these two cases depends on the schedule of the United States District Court. All of the 4,529 subrogation claims have been processed, and 70 percent of each of those claims has been paid, leaving $34,509,270 as the remaining subrogation liability. The subrogation claims will be paid with funds remaining after the adjudication of the two claims in Federal Court.

PRE-DISASTER MITIGATION GRANTS

Question. Last year the Conferees expressed concern over the slow progress in awarding fiscal year 2003 Pre-disaster Mitigation Grants and over the unobligated balances that remained in the program. How much fiscal year 2004 funding has been released to date and how much remains unobligated in the program?

Answer. To date, FEMA has not released any fiscal year 2004 competitive grant funding ($131 million). Since the PDM funds are available until expended, FEMA is combining the remaining fiscal year 2003 funds with the fiscal year 2004 funds and with the fiscal year 2005 appropriation into a streamlined fiscal year 2005 PDM competitive grant program. Of the fiscal year 2004 appropriation of $149 million, a total of $137 million (competitive grants, administrative, and miscellaneous funding) remains unobligated.

Question. For fiscal year 2005 funds, why is it taking so long to distribute the funds and how can the program be expedited?

Answer. After completing the first competitive PDM process, FEMA began awarding the fiscal year 2003 grants in April 2004. The fiscal year 2003 appropriation, authorized in February 2003, directed FEMA to implement a PDM grant program in three parts: (1) a nationally competitive PDM grant program for state, territory, local government, and Indian tribal government projects and plans; (2) a nationally competitive PDM grant program for disaster-resistant university projects and plans; and (3) a one-time planning grant allocation to the states and territories. The PDM grants are awarded based on the results of a three-phase competition—eligibility and completeness review, technical evaluation, and national evaluation team review. The applications are ranked and announced, and subsequently, the applicants are notified that their application has been selected for funding. Once this takes place, the grant award process can begin. The majority of the fiscal year 2003 funds have been awarded; however, an additional $18.5 million will be awarded when ongoing Federally required environmental and historic preservation compliance reviews are complete. FEMA anticipates that this will be no later than the end of fiscal year 2005. At that point, FEMA will have funded all eligible fiscal year 2003 grant applications and approximately $11 million in fiscal year 2003 funds will remain.

In response to the announcement of funds available for fiscal year 2005, FEMA received 821 applications totaling nearly $517 million. FEMA conducted eligibility and completeness reviews in March 2005. Technical reviews in the areas of engineering, cost effectiveness, and environmental and historic preservation were conducted in March and April 2005. The National Evaluation will be conducted May 17-June 3, 2005. Representatives from 27 states, 3 tribes, and 1 territory will participate in the National Evaluation process.

Based on the eligibility, completeness, and technical reviews completed to date, FEMA expects that the selection of grants for award will be completed in June, after which pre-award activities and the obligation of grant awards will begin. Grants will be selected so that ultimately, all funds from fiscal year 2005 and prior years will be obligated.

Federal environmental and historic preservation compliance requirements for project grants, as well as state-level grant processing requirements, are significant factors that can delay the obligation of grant funds to selected grantees. FEMA will work with grantees to complete these requirements expeditiously; however, for those grants that cannot be obligated in fiscal year 2005, FEMA will work to complete the requirements and to obligate the grant funds as early as possible in fiscal year 2006.

FEMA PERSONNEL

Question. Recently FEMA has experienced a large number of vacancies. In fiscal year 2004 and to date in fiscal year 2005 how many vacancies has FEMA experienced in headquarters and in the regions?

Answer. At the end of fiscal year 2004, there were approximately 357 vacancies agency-wide (not including Stafford Act employees). By mid-year of fiscal year 2005, FEMA had approximately 342 vacancies agency-wide.

Question. Were any of those vacancies eliminated or transferred to other parts of DHS?

Answer. Yes, some of the vacancies were transferred to the SLGCP at the start of fiscal year 2005.

Question. Is so, what is the total number eliminated, and the total number transferred and to where?

Answer. Sixteen vacancies were transferred to SLGCP at the start of fiscal year 2005.

Question. How many vacancies does FEMA have as of April 20, 2005?

Answer. As of April 20, 2005, FEMA has approximately 342 vacancies.

Question. What is the current plan at FEMA for filling vacancies?

Answer. FEMA will continue to fill vacancies and to maintain staffing levels sufficient to sustain its mission.

Question. How has the vacancy of so many positions affected the ability to prepare and respond to disasters?

Answer. FEMA still is able to maintain its mission capability.

IA'S ROLE IN INTELLIGENCE COMMUNITY

Question. In February 2004, the DHS IG noted that the mission of the IAIP Risk Assessment Division (RAD) overlaps in many ways with the Terrorist Threat Integration Center (TTIC), now called the National Counterterrorism Center. The TTIC was created through executive order in 2003. In August 2004, the IG noted that DHS is not playing a lead role in consolidating terrorist watch list information even though the Homeland Security Act called for DHS to play a major role in watch list consolidation. In December of 2004, the Intelligence Reform and Terrorism Prevention Act was signed by the President making sweeping changes in the intelligence community.

With the Intelligence Reform Act and other executive orders stripping away most of the responsibilities of IA and placing them with the National Counterterrorism Center (NCTC) and the Terrorist Screening Center, what role does IA play in the intelligence community?

Answer.

The Role of DHS Office of Information Analysis in the Intelligence Community

DHS Office of Information Analysis (IA) plays a leading role in the intelligence community for homeland security intelligence. The Office provides border, infrastructure, maritime and domestic threat analysis; fuses unique information from our components and our non-traditional stakeholders; and serves as the primary intelligence information provider to state, local, territorial and tribal governments and the private sector, as well as their advocate for intelligence information within the intelligence community. As I announced on July 12, 2005, I am committed to enhancing this role.

DHS IA's role as a leader of homeland security intelligence within the intelligence community is likewise enhanced by the IRTPA 2004 and other executive orders; the greater integration of the intelligence community as a result of IRTPA 2004 will strengthen the ability of DHS IA to carry out its mission.

IRTPA 2004 and the Integration of the Intelligence Community

DHS IA is aggressively integrating into the intelligence community to ensure we can maximally contribute to the nation's security, especially in our unique areas of expertise (producing unique analysis and providing unique information), and to ensure we are able to most effectively leverage the expertise and support of the intelligence community on behalf of the Homeland Security mission and its stakeholders, especially those non-traditional stakeholders such as State, local, territorial, and tribal governments and the private sector (with whom we have unique partnerships).

Integrating DHS IA Unique Analytic Expertise into the Intelligence Community

DHS IA has "forward deployed" DHS intelligence analysts to our intelligence community partners, to include the National Counterterrorism Center (NCTC), the Federal Bureau of Investigation, and to non-intelligence community members such as the TSC.

These seasoned analysts are able to ensure our intelligence community partners have the benefit of our unique DHS analytic expertise in Border Security Intelligence, Infrastructure Security Intelligence, Maritime Security Intelligence (esp. through our Homeland Infrastructure Threat and Risk Assessment Center), and Domestic Threat Intelligence.

We frequently collaborate with our partners when expertise is required in our unique analytic areas and we are fully engaged in ongoing community efforts to develop community production plans reflective of an efficient application of the community's resources. For example, DHS IA is fully participating in the NCTC led effort to develop a communitywide counterterrorism production plan; we are taking the lead in those areas that make use of our unique DHS analytic areas (borders, infrastructure, maritime and domestic threat, as appropriate) and partnering with other organizations on those topics that will be strengthen by including our experts' input.

Working with NCTC and TSC on Analysis

DHS IA has been a strong partner in NCTC since its inception as the Terrorist Threat Integration Center in January 2003. On a daily basis we levy the expertise resident in the NCTC to answer the needs of our customers—we focus on ensuring the best counterterrorism analysis in the government is put into a form, context and classification that is useful for our state, local, territorial and tribal governments and private sector partners. At the same time, we provide our substantial expertise to the NCTC on areas where we are the experts: borders, infrastructure, maritime, and domestic threat analysis. The result of this partnership is that we work together on many joint products—bringing the best expertise in the government to bear on behalf of our customers.

DHS IA took a lead role in helping stand up the TSC, providing staff and support (to include a senior manager). Our experienced analysts in the TSC help ensure the success of its vital work in watchlist consolidation.

DHS IA also conducts a valuable alternative analysis program; our Red Cell provides alternative analytic perspective to complement—and challenge—NCTC and others findings. Our Red Cell has received compliments for its insightful and adventurous thought—and this work is an essential component of the alternative analytic capability required under IRTPA 2004.

Integrating DHS IA Unique Information into the Intelligence Community

In parallel with our efforts to integrate DHS unique analytic expertise into the intelligence community, we are also moving forward in ensuring our vast DHS unique information holdings are made available to the intelligence community through direct access and quality reporting.

DHS has vast information holdings, unique to this department, either as a result of our operational elements' investigations and enforcement operations or as a result of our unique position as the primary interface between the Federal Government and the State, local, territorial and tribal governments and private sector.

DHS IA is working to ensure analysts throughout the intelligence community have access to our information holdings, while respecting the privacy and civil liberties of our citizens. In several cases, the Department has made operational elements' data holdings directly available to partner organizations in the intelligence community. In addition, DHS IA is establishing a reports officer program, focused on drawing information out of the department's information holdings and placing them into traditional intelligence community channels, through the Intelligence Information Reports vehicle. DHS IA has deployed trained reports officers into key departmental operational nodes to report counterterrorism information derived from border enforcement efforts and immigration investigations to the intelligence community. In the future, DHS IA will deploy trained reports officers throughout the components—and out into State and Local Fusion Centers—to ensure the all the department's relevant information is made available to those who need it, in a timely manner and in the channels analysts in the intelligence community are comfortable with and expect to receive reporting.

Integrating DHS IA Unique Partnerships into the Intelligence Community

DHS IA has been charged to be the primary Federal Government intelligence information provider to the State, local, territorial, and tribal governments and the private sector (a responsibility re-emphasized by IRTPA 2004)—and to be their advocate within the intelligence community. On a daily basis we are integrating our support for these customers into the larger intelligence community by working to ensure the free flow of information and products from the intelligence community out to our customers, by providing actionable intelligence, and by contextualizing intelligence to explain the product to our customers in terms they understand and working with our partners to produce the reports at the classification levels our stakeholders can use.

We are also continually working to ensure our customers' requirements—whether they are for information or for finished analytic production—are represented in the intelligence community requirements statements, collection decks, and production plans. Our work in integrating the homeland security intelligence requirements of the state, local, territorial, and tribal governments and the private sector into the intelligence community requirements system is the first time these requirements have been systematically included and advocated for in the intelligence community.

IRTPA 2004 and DHS IA Departmental Responsibilities

In addition to our lead role for homeland security intelligence within the intelligence community, DHS IA maintains several key departmental support respon-

sibilities—including a new role of leading and managing the departmental intelligence activities.

Some of these key departmental roles include:

—Providing direct support to the Secretary and department senior staff for policy, programmatic, and operational decision making.

—Developing the plans, programs and policies required to build a unified, integrated DHS intelligence capability, which the Secretary has said will lie at the heart of the department's risk-based approach to securing the homeland.

—Supporting the Homeland Security Advisory System (HSAS). IA will continue to provide specific intelligence to the Secretary and the White House to enable timely changes in the threat level and support dissemination of this information to stakeholders. We will contribute to the function of Indications & Warning (I&W) in partnership with the HSOC.

—Building out of the intelligence infrastructure for DHS headquarters.

—Developing an Education, Training, and Career Workforce Management Program for DHS analysts and intelligence professionals.

Finally, early reviews by the DHS OIG and concerns resulting from the changing roles and responsibilities of the NCTC and other organizations due to IRTPA 2004 and other executive orders are not reflective of the successes DHS IA has demonstrated as a leader within the intelligence community for homeland security intelligence. As stated above, our value added comes in our unique data and analytic expertise (border, infrastructure, maritime, and domestic threat analysis—analysis that has distinguished itself on several occasions and led the community toward the appropriate threat characterization), in providing our unique information (information never before available to the intelligence community and by which we have already contributed to successes in other agencies), and in partnering with our stakeholders—especially in our unique role as the primary Federal Government intelligence information provider to the state, local, territorial, and tribal governments and the private sector and in our role as their advocate within the intelligence community.

We remain focused on our mission of leading the DHS intelligence activities in support of the department and its components, and for the full benefit of the state, local, territorial, and tribal governments and the private sector, to secure the homeland, defend our citizenry, and protect our critical infrastructure.

Question. What role does the Homeland Security Operations Center (HSOC) serve in comparison to the NCTC?

Answer. In contrast to the NCTC, the HSOC provides general domestic situational awareness, a common operational picture, and support to the IIMG and DHS Leadership, as well as acting as the primary conduit for the White House Situation Room and IIMG for domestic situational awareness. The HSOC will continue to collect domestic related suspicious activity reports, look at domestic terror threats and natural disasters, focusing efforts domestically. HSOC is the lead conduit to State and local agencies.

Question. The FTE levels authorized for IAIP appear to be based on the larger role in intelligence gathering and analysis that was envisioned when IAIP was established. What is the justification to carry such a high number of FTE for intelligence analysis now that many functions envisioned by the Homeland Security Act have been placed at other agencies?

Answer. IAIP's mission is an entirely new one, and it is a manpower-intensive effort owing to the vast size and scope of the threats to the homeland. IAIP is performing an intelligence mission never before attempted, and it is a mission that includes Federal, state, local, tribal entities as well as privately-held interests. Additionally, IAIP is responsible for intelligence pertaining to securing the borders of the United States, which is in itself an enormous undertaking. DHS and IAIP have been given the mission of producing intelligence analysis and products that simply did not exist before, and to do so with a "target set" that is staggering in its size and complexity. While the need to conserve resources is clear, the need to perform the analyses needed to ensure that our Homeland is prepared to detect, intercept, withstand, and, if necessary, recover from a terrorist attack is even more vital.

CHEMICAL SECURITY

Question. Last year, I asked Secretary Ridge about his plans to address security at chemical plants and he told me that the private sector was taking care of it. Yet, the Department has no benchmarks to determine whether the private sector is taking steps to secure its facilities. In response to this apparent gap in our security, last year, I asked GAO to determine what steps are being taken by the private sector to protect the American people. The GAO concluded that for 93 percent of the

industry, it is uncertain whether facilities are improving security at all. Only 1,100 of the 15,000 chemical facilities identified by the Department of Homeland Security are known to adhere to voluntary industry security procedures.

It has been more than 2 years since the GAO urged the EPA and DHS to develop a comprehensive strategy for the protection of our chemical plants. Yet, little has been done.

What are your plans to enhance security for the chemical sector?

Answer. As part of the development of the NIPP, the Office of Infrastructure Protection (IP) has been tasked with authoring the Chemical Sector Specific Plan (SSP), which will outline the strategic guidance for securing the Chemical Sector.

While the Chemical SSP is being developed, DHS continues to work within the Chemical Sector to enhance overall protective capability through several ongoing initiatives. To help guide the resource targeting of these initiatives, the Department is applying a risk management process that examines the likelihood of a given event and its potential consequences. This approach allows for the Department's protective efforts to be directed at those chemical facilities posing the greatest potential danger to the American public. Examples of these protective efforts include the following:

—*Site Assistance Visits (SAVs).*—SAVs are visits to critical infrastructure facilities by DHS protective security professionals in conjunction with subject-matter experts and local law enforcement (LLE) to assist asset owner/operators in assessing vulnerabilities at their facilities. To date, SAVs have been conducted at 38 chemical facilities.

—*Buffer Zone Protection Plans (BZPPs).*—BZPPs identify and recommend security measures for the area surrounding a facility (the "Buffer Zone"), making it more difficult to plan or launch an attack. DHS trains LLE personnel on how to assess Buffer Zone security and provides a standardized template for use in the creation of a BZPP. To date, DHS has received BZPPs for 111 chemical facilities, with BZPPs expected to be completed for the 289 highest-risk chemical facilities by the end of fiscal year 2005. In conjunction with the BZPP program, $14.5 million in grants have been provided to first preventers responsible for the protection of chemical facilities

—*Educational Reports.*—Based on data gathered from SAVs and BZPPs, DHS has developed three types of educational reports for use by LLE and asset owner/operators to learn how to better secure CI/KR assets. Characteristics and Common Vulnerabilities reports (CVs) identify common characteristics and vulnerabilities at specific types of CI/KR. Potential Indicators of Terrorist Activity reports (PIs) provide information on how to detect terrorist activity in areas surrounding CI/KR. Protective Measure (PM) reports identify best practices and other protective measures for use at specific CI/KR types. CVs and PIs have been developed for Chemical Facilities, Chemical Storage Facilities, and Chemical and Hazardous Materials Transportation. A PM report has been developed for the Chemical and Hazardous Materials Industry.

—*Facility Security Assessments/Facility Security Plans (FSAs/FSPs).*—Pursuant to the Maritime Transportation Security Act of 2002 (MTSA), owners of chemical facilities located along waterways are required to complete FSAs and FSPs and submit them to the USCG for review and approval. FSPs must include security measures and procedures for responding to security threats. To date, USCG personnel have visited over 230 chemical facilities under the MTSA.

—*Risk Analysis and Management for Critical Asset Protection (RAMCAP).*—DHS, in conjunction with the American Society for Mechanical Engineers, is developing the RAMCAP, a risk assessment methodology that will allow asset owners/operators to assess the security of their critical assets. Results from RAMCAP assessments will allow comparison of assets from across sectors, allowing for better prioritization of national CI protective efforts. The Chemical Sector module will be completed by the end of the second quarter of fiscal year 2005.

—*Webcams.*—Web-based cameras have been installed at ten high-risk chemical facilities in order to enable LLE and DHS to conduct remote surveillance of the buffer zone surrounding each facility during elevated threat levels.

—*Tabletop Exercises.*—As part of DHS-IP's Exercise Program, tabletop exercises have been conducted at six chemical facilities. The findings from these exercises are compiled in After Action Reports which serve as a basis for planning future exercises; upgrading security plans and operating procedures; and taking corrective actions.

—*TIH Rail Security.*—DHS, in conjunction with DOT, is supporting a variety of efforts to improve security for Toxic-by-Inhalation Hazards (TIH) rail shipments. These efforts include studying ways to make HAZMAT rail cars less identifiable; conducting vulnerability assessments for the high-risk urban areas

where the largest quantities of TIH chemicals move by rail; a DC Rail Pilot Project involving a "virtual fence" with various sensors and monitors to help secure the DC rail corridor from potential incidents involving HAZMAT; and establishing TIH HAZMAT teams in the DC area.

—*Training.*—DHS provides various training courses to asset owner/operators, State and local government officials, and LLE agencies responsible for the protection of chemical facilities. Such courses include: Terrorism Awareness and Prevention; Advanced Bomb Technician Training; Surveillance Detection; SWAT Operations; and Underwater Hazardous Device Search Training.

—*Private Sector Initiatives.*—In addition to protective activities led by DHS or other Federal entities, asset owner/operators in the Chemical Sector are voluntarily undertaking a variety of security initiatives. Chief among these is performance of self-assessments using the Responsible Care® Security Code (Security Code). This code, developed by one of the Chemical Sector's largest trade associations, is designed to help chemical facilities improve their security using a risk-based approach to identify, assess, and address vulnerabilities; prevent or mitigate incidents; and enhance training and response capabilities. Implementation of the Security Code is a prerequisite for membership in some of the sector's largest industry associations. Recently, DHS reached a tentative third party verification agreement with two of these associations (the American Chemistry Council and the Chlorine Institute).

Question. Will legislation be proposed to Congress that sets security standards across the industry?

Answer. At this time, our non-regulatory partnerships with industry are producing results. However, DHS has concluded that the existing patchwork of authorities does not permit us to regulate the industry effectively. Accordingly, DHS has agreed to work with Congress to assess the need for a carefully measured, risk-based regulatory regime in the chemical sector designed to close the existing gaps and develop enforceable performance standards to reduce risk across the chemical sector.

Question. Do you agree that the Department must establish benchmarks to assess both the private sector's and Federal Government's role in securing the chemical sector?

Answer. DHS believes facility chem site security should be based on reasonable, clear, equitable performance standards. Enforceable performance standards should be based on the types and severity of potential threats posed by terrorists, and facilities should have the flexibility to select among appropriate site-specific security measures that will effectively address those threats.

BUFFER ZONE PROTECTION PLANS

Question. DHS recently released $92 million in Buffer Zone Protection Plan grants. Of the 1,849 grants, provide a chart that shows the distribution of grants and the funding by critical infrastructure sector.

Answer. Please see table below.

BREAKDOWN OF BZPPS BY SECTOR FOR FISCAL YEAR 2004–2005

SECTOR	Number of sites [1]	Percent of sites	Approx. funding [2]
Agriculture & Food	5	0.27	$250,000
Banking & Finance	41	2.20	2,050,000
Chemical & Hazardous Materials Industry	272	14.62	13,199,870
Commercial Assets	880	47.29	43,592,631
Dams	7	0.38	350,000
Defense Industrial Base	6	0.32	300,000
Emergency Services	5	0.27	202,975
Energy	213	11.45	10,550,954
Government Facilities	142	8.28	7,100,000
Information Technology	5	0.27	250,000
National Monuments & Icons	10	0.54	500,000
Nuclear Power Plants	92	4.94	4,423,802
Postal Shipping	2	0.11	100,000
Public Health	23	1.24	1,117,506
Telecommunications	5	0.27	250,000
Transportation	98	5.27	4,836,168
Water	43	2.31	2,150,000

BREAKDOWN OF BZPPS BY SECTOR FOR FISCAL YEAR 2004–2005—Continued

SECTOR	Number of sites [1]	Percent of sites	Approx. funding [2]
TOTALS	1,849	100.00	$91,223,906

[1] The exact composition of the fiscal year 2004–05 BZPP list is still evolving; the current sector breakout is a snapshot, but will not change substantially.

[2] Subject to prioritization decisions of 18 States and 1 territory that have elected to prioritize their assets, an exact sector breakdown is not currently available. A total of $91,315,793 is available under the grant program.

Question. Does DHS plan to broaden the criteria for receiving grants to include the gross consequence of an attack and other vulnerabilities?

Answer. In determining where to target its protection resources, DHS applies a risk management process that examines the likelihood of attack and its potential consequences. This approach allows the department's protective efforts to be directed at those facilities posing the greatest potential danger to the public. DHS is continuing to improve data collection in support of risk analysis, and to refine our risk assessment methodologies to ensure resources are being spent where they are most needed.

MANAGEMENT & ADMINISTRATION

Question. The fiscal year 2006 congressional justification shows that $1 million will be spent on "Purchases from Government Accounts" and $19 million for fiscal year 2006. In response to reprogramming questions, IAIP adjusted the number for "Purchases from Government Accounts" to $20.2 million. Provide a detailed chart on what the $20.2 million will buy in fiscal year 2005 and what the $19 million will buy in fiscal year 2006.

Answer. In fiscal year 2005, the reprogramming of $20.2 million into "Purchases from Government Accounts" includes funding for facilities, Project Management Office, and IT costs. In fiscal year 2006, the $19 million in "Purchases from Government Accounts" will fund the Homeland Secure Data Network (HSDN).

Fiscal year 2005:	
Homeland Secure Data Network	$7,500,000
Shared Services	2,000,000
Facilities	4,500,000
WCF Contribution	7,700,000
IT NCR ops	500,000
Total	22,200,000
Fiscal year 2006: Homeland Secure Data Network	19,400,000

Question. Explain the large increases in fiscal year 2006 for equipment and land and structures.

Answer. The $38 million funding request does not support the design and construction phases of facilities projects. Department Operations requests funds for the facilities design, basic tenant improvements (construction/renovation), physical security upgrades, and emergency power requirements for facilities IAIP will occupy at the Nebraska Avenue Complex (NAC). The IAIP facilities funding is requested to support the costs of occupying facilities, both on and off the NAC, once they are ready, including fit out costs such as furniture, computers and other Information Technology (IT), and the operations and maintenance costs (rent, security, IT support) associated with occupied facilities. Specifically, the operations and maintenance portion of the IAIP facilities funding covers electric costs for additional air conditioning required due to the technology requirements in IAIP spaces (HSOC and server requirements), maintenance for the secure, up to date unclassified and classified Local Area Networks, IT desktop services, as well as required janitorial services. The tenant improvement portion of this funding covers the mentioned fit out costs and ensures facilities capable of meeting both the classified and unclassified space and technology requirements in recognition of the fact that IAIP is an IT and security intensive tenant. These costs include IT infrastructure and cabling, IT equipment, security, IT certification and accreditation, furniture, data migration and relocation costs. The request does not pertain to land, as IAIP is a tenant in GSA-controlled facilities.

CONTRACT EMPLOYEES

Question. In response to fiscal year 2005 reprogramming inquiries, IAIP reported that there are 564 contractors supporting the program function of IAIP, 138 of which are funded through the Management & Administration account and 426 through the Assessments and Evaluations Account.

Of the 426 in the A&E account, what is the distribution of contract support by portfolio?

Answer. Please see chart below.

Account	Contract support
Management & Administration	138
Assessments and Evaluations	426
Homeland Security Operations Center	32
Critical Infrastructure Outreach and Partnerships	74
Cyber Security	78
NS/EP Telecommunications	32
National Infrastructure Simulation and Analysis Center; Protective Actions; Critical Infrastructure; Identification and Evaluation; Biosurveillance	24
Threat Determination and Assessment; Evaluations and Studies; Infrastructure Vulnerability and Risk Assessment	186
Total	564

Question. What makes these positions not inherently governmental positions?

Answer. The support personnel listed against the programs are performing services consistent with Appendix B to Office of Federal Procurement Policy (OFPP) policy letter 92–1. On-site contractor personnel only perform support functions to IAIP and do not perform any activities that are considered inherently governmental. IAIP is currently covering significant portions of the workload associated with open authorized FTE positions (which are inherently governmental) through significant workload sharing of on-board FTE and use of contractors to support non inherently governmental functions of those same FTEs. The mix of contractor support staff will change as programs progress and as new tasks are levied, and workloads will redistribute to more logical and efficient workflows as FTEs come on-board. Although the current work flow arrangements are difficult, they are working due to the dedication and professionalism of the current FTE workforce. IAIP is aware of its responsibilities under the FAIR Act (A–76) and we annually review functions for inherently governmental versus commercial activities.

ASSESSMENTS AND EVALUATIONS

Question. The budget request shows—$137.404 million in Adjustments to Base. For each adjustment on page 76 of the congressional justification for IAIP, explain the reduction or increase.

Answer. Please note that all dollars are in thousands.

CRITICAL INFRASTRUCTURE IDENTIFICATION AND EVALUATION

Description	Adjustment
A decrease of $4,789 is due in part to contractor savings created by the increased number of FTE positions for Field Security Detachments. Additionally, further savings are garnered by the joint funding of Protective Security Task Forces (PSTFs) between Critical Infrastructure Identification and Evaluation (CIIE) and Public Actions (PA). There are elements of the PSTF program that align with CIIE such as the identification of critical infrastructure and the CI/KR expertise of the PSTF team members. However, the overarching emphasis of the PSTF mission is the implementation of protective measures at high priority CI/KR in light of emerging threats. In fiscal year 2006 the program will be funded jointly between CIIE and PA, but the entire program will be transitioned to PA in fiscal year 2007. This is an attempt of IP to better align our programs with the budget structure	($4,789)
A decrease of $899 will be transferred to S&T to support Supervisory Control and Data Acquisition Testing within Cyber Security, responsible for securing the U.S. industrial systems that have become increasingly dependent on powerful, electronic communications tools, the internet, and supervisory control and data acquisition (SCADA) systems	(899)
Total Adjustments to Base	(5,688)

NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER ADJUSTMENTS TO BASE

Description	Adjustment
Travel, includes all costs of transportation of persons, subsistence of travelers, and incidental travel expenses in accordance with Federal travel regulations. In fiscal year 2004 travel for Headquarters personnel was funded from M&A, but has been transferred to A&E for fiscal year 2005 and fiscal year 2006	($5)
Advisory and Assistance Services; the fiscal year 2006 request includes decreases due to decreases in program advisory services and transfers of shared service expenses from A&E back to M&A	(3,995)
Total Adjustments to Base	(4,000)

BIOSURVEILLANCE ADJUSTMENTS TO BASE

Description	Adjustment
Technical Adjustments	$147
Total Adjustments to Base	147

PROTECTIVE ACTIONS ADJUSTMENTS TO BASE

Description	Adjustment
In fiscal year 2006, the PA program is reduced by $53,000 to establish the new TIP program administered by the SLGCP. TIP grants will be used by state/local/territorial/tribal entities to procure goods and services determined necessary by IAIP's BZPP process. Previously, these goods and services which reduce the vulnerability to terrorist threats around certain high vulnerability critical infrastructures and key assets within the state/local/tribal jurisdiction were funded by assistance from IAIP. The TIP program will also result in a $3,000 savings in program consultation support costs	($53,000)
A decrease of $41,500 for Emerging Pilot Projects and Technology Application Pilots saving initiative	
Technology pilots will be a cooperative effort with S&T for the development of new technologies for protective measures. This effort is funded within S&T	
Emerging Pilot Projects has evolved into the Protective Measures Demonstration Pilots project which takes advantage of innovative uses of existing protective methods and commercially available equipment and technology to enhance the security of CI/KA	
A pilot project would take technology already developed for a specific use and apply it to fill gaps in protective security and evaluate the effectiveness and benefits in ''real life'' or field environments as they relate to IP objectives and priorities. Protective Security Pilots are developed from gaps and protection shortfalls identified in interdependency analysis and consequence of attack analysis as directed by the NIPP, and also from BZPPs, SAVs, and needs identified by Sector Specific Agencies. Pilots are meant to demonstrate solutions for vulnerabilities that cross sectors and stakeholders. Once the means of mitigating the vulnerability is established and proven, the solution is disseminated to all entities that have similar vulnerabilities so that the strategies can be integrated in their respective risk management strategies	
IP is the Sector Specific Agency for 3 sectors (chemical, nuclear, and commercial assets) and is also responsible for cross-sector protection as detailed in the National Infrastructure Protection Plan. IP is responsible for increasing the general level of protection for CI/KR sites absent of specific threat and is also responsible for addressing specific threat events. PSD's intention in fiscal year 2006 is to address the most critical vulnerabilities identified by vulnerability assessments and BZPPs in fiscal year 2005 within the sectors that IP is directly responsible for, including chemical, nuclear and commercial sectors. Other individual sectors and cross-sector vulnerabilities will also be addressed with the demonstration of pilot protective measures based on intelligence and threat information. As directed by the National Infrastructure Protection Plan (NIPP) and HSPD–7, demonstration pilots are also taken on by PSD to mitigate specific vulnerabilities across sectors as the dynamic threat environment changes	(41,500)
A Decrease of $9,800,000 for Regional Protective Actions	
Pilot programs to establish regional centers for use by local law enforcement entities will not be continued in fiscal year 2006. The performance impact will be negligible as PSD will maintain close contact with local police and protective security agencies through the use of the outreach program, training programs, Site Assistance Visits, the BZPP program and visits by Protective Security Advisors and other DHS personnel. DHS also conducts seminars and conferences in order to maintain contact with State and local agencies. PSD has developed close working relationships with local police agencies and will continue to foster and maintain these relationships in the future	(9,800)
Technical Adjustments	4,052

PROTECTIVE ACTIONS ADJUSTMENTS TO BASE—Continued

Description	Adjustment
Total Adjustments to Base	(100,248)

CRITICAL INFRASTRUCTURE OUTREACH AND PARTNERSHIPS ADJUSTMENTS TO BASE

Description	Adjustment
Technical Adjustments	$885
The cost of maintaining the data center which was funded in fiscal year 2005, in the CIOP program, and initiated under the direction of the Department's CIO is not requested in fiscal year 2006	(35,000)
A $13,800 reduction in CIOP results from a restructuring and completion of analytical tasks, institutionalization of partnership relationships, and implementation of management efficiencies	(13,800)
Total Adjustments to Base	(47,915)

CYBER SECURITY ADJUSTMENTS TO BASE

Description	Adjustment
Technical Adjustments	$969
Total Adjustments to Base	969

NS/EP TELECOMMUNICATIONS ADJUSTMENTS TO BASE

Description	Adjustment
Advisory and assistance services includes services to support Executive Order 12472, which provides authority for the National Communications System (NCS) to initiate telecommunications service priority programs such as Wireless Priority Service (WPS) and Government Emergency Telecommunications Service (GETS). GETS and WPS are essential telecommunications services to support restoration and recovery following catastrophic events	$1,807
Travel	57
Technical Adjustments	14
Total Adjustments to Base	1,878

THREAT DETERMINATION AND ASSESSMENT ADJUSTMENTS TO BASE

Description	Adjustment
Information can be provided under separate cover upon request	($2,043)
Total Adjustments to Base	(2,043)

INFRASTRUCTURE VULNERABILITIES & RISK ASSESSMENTS ADJUSTMENTS TO BASE

Description	Adjustment
Information can be provided under separate cover upon request	$3,267
Total Adjustments to Base	3,267

COMPETITIVE ANALYSIS AND EVALUATION ADJUSTMENTS TO BASE

Description	Adjustment
Information can be provided under separate cover upon request	($4,000)
Total Adjustments to Base	(4,000)

EVALUATIONS AND STUDIES ADJUSTMENTS TO BASE

Description	Adjustment
Information can be provided under separate cover upon request	$20,139
Total Adjustments to Base	20,139

HOMELAND SECURITY OPERATIONS CENTER ADJUSTMENTS TO BASE

Description	Adjustment
Technical Adjustments	($192)
Total Adjustments to Base	(192)

INFORMATION SHARING AND COLLABORATION ADJUSTMENTS TO BASE

Description	Adjustment
Technical Adjustments	$282
Total Adjustments to Base	282

Question. The budget proposes a decrease of $41.5 million for Emerging Pilot Projects and Technology Application Projects with the understanding that "this effort is funded within S&T." There is no budget transfer into S&T for this purpose. Is this just a simple reduction in this area?

Answer. The Emerging Pilot Projects and Technology Application Projects are designed to review existing technologies and help get appropriate protective measures in the field in a usable manner. These pilots and projects identify commercially available or emerging technologies and determine if they can be successfully used to eliminate existing vulnerabilities in a real-world situation. These projects will allow DHS to expand the potential protective measures that can be deployed and to fill existing identified operational gaps. The Technology Application Projects identify commercially available technology and determine if the technology can be applied in the field to fill real needs. The Emerging pilots are required to ensure that any new technology is deployed to the field with appropriate methods and restrictions to allow the state, local, or commercial operators to successfully implement the new technologies. Aspects for successfully technology deployment require: pilots to determine the usefulness of a technology under various conditions; personnel training for deployment and effective use; monitoring methods or personnel required; required response time; technology calibration information; maintenance cycle and manuals, etc.

NOAA WEATHER RADIOS

Question. Virtually none of the funding appropriated for NOAA radios as been obligated by IAIP. Why does this funding remain unobligated?

Answer. IAIP has obligated the procurement and shipment of NOAA "All Hazard" radios to schools across the country. Specifically, a $500,000 pilot program has been funded to disseminate these radios to all the K–12 public schools in certain UASI cities and two rural states. The radios will arrive in September, which coincides with the start of the school year and National Preparedness Month. These radios regularly disseminate weather related information and can now broadcast official DHS alert and warning information. (DHS/IAIP and Commerce/NOAA entered into a MOA in 2004 that provides for DHS message dissemination over NOAA's All Hazard Radio and also over FEMA's local Emergency Alert System.) IAIP, NOAA, Department of Education, DHS Citizen Corps, DHS Procurement, DHS Grants Office, and other DHS entities have been in regular contact regarding this effort for over a year. After lessons have been learned from this initial pilot, additional IAIP alert and warning funds ($1.5 million) will be used for radio procurement for other schools across the country. This $2 million obligation for the radios and the $18 million transferred to FEMA for program management of other alert and warning projects represent all IAIP funding to improve alert and warning for the general public.

VIOLATING THE DHS APPROPRIATIONS ACT

Question. Congress and this Committee take very seriously the constitutional powers bestowed on the legislative branch to enact laws. Article I, Section 9, Clause 7 States that "No money shall be drawn from the Treasury but in Consequence of Appropriations made by law."

Since the beginning of fiscal year 2005, the Department, on several occasions, has violated legislative provisions set forth in the fiscal year 2005 Homeland Security Act. For example, Section 503 of the Act sets strict reprogramming and transfer guidelines restricting the ability of the Department to reallocate appropriated dollars from one program to another without congressional notification. In fiscal year 2005, DHS has violated that provision on more than one occasion. In one instance, DHS stood up a brand new office, called the Domestic Nuclear Detection Office, which has been reporting directly to the Secretary. The start-up costs for this office were taken from funds appropriated to the Under Secretary for Science and Technology. Within the Information Analysis and Infrastructure Protection Office, the Department reallocated funding from an appropriation that pays salaries to its employees to start a new program called Information Sharing and Collaboration. Section 507 of the fiscal year 2005 Act requires DHS to notify Congress on any contract or grant in excess of $1 million 3 business days before it is announced. This provision is an important tool for Congress to keep track of the vast amount of contract and grant funding appropriated to the Department. On several occasions, the Committee has become aware of grants or contracts through the press after the award had been made and without a notification to Congress. In addition, the S&T Directorate spends the majority of its $1 billion annual appropriation on R&D contracts and grants. Through January 31 of this year, the S&T Directorate expended nearly $120 million, yet the Committee has received only 1 grant notifications and 1 contract notification.

Mr. Secretary, I don't expect that you were apprised of these violations nor will you be able to comment on them today. My questions is however, will you look into this pattern of negligence and develop a plan within your office to ensure that the Department will follow the letter of the law as enacted by the U.S. Congress and signed by the President of the United States? As part of your transition review, will you develop a plan to avoid other violations similar to the examples I described?

Answer. The Department takes seriously its responsibility to adhere to the reporting requirements referred to in this question. One of the key imperatives that will drive this Department is to improve DHS' stewardship, particularly with respect to financial management. Likewise, improving communications with Congress, including the timely provision of information such as reports and reprogrammings are important, and will be improved. The Department has already put in place new mechanisms to better track and more aggressively manage reports assigned to DHS by Congress. DHS considers this an important priority and is dedicating significant focus and attention toward ensuring reports are sent to Congress in a timely manner. With respect to the DNDO, the Department provided a reorganization notification and a reprogramming notification, and withheld spending resources for any DNDO activities, including the setting up a DNDO, during the required waiting period. Congress repeated this message in its action on the supplemental in May, and the Department has abided by the requirements and deadlines in that bill and report.

QUESTIONS SUBMITTED BY SENATOR PATRICK J. LEAHY

IMMIGRATION AND CUSTOMS ENFORCEMENT

Question. Immigration and Customs Enforcement (ICE) has been plagued by budget problems basically since the creation of your department. ICE has had a hiring freeze in place since last year and it is unclear when it will be lifted, and only a significant reprogramming request allows it to balance its books for the current fiscal year. Of course, these funding problems are occurring while members of Congress from both parties have emphasized the importance of enforcing our immigration laws in the interior.

How will you ensure that ICE has the funding it needs to perform its mission?

Answer. I am committed to ensuring that ICE has the funding it needs to perform its mission. The fiscal year 2006 President's Budget, which includes $205 million to address base requirements within the agency, along with fiscal year 2005 supplemental funding, will assure that ICE has the necessary funding.

Question. Does the Administration's fiscal year 2006 request provide sufficient funds to avoid another large reprogramming request next year?

Answer. The fiscal year 2006 request provides sufficient funds to avoid another large reprogramming request in fiscal year 2006.

ALL-STATE MINUMUM

Question. I was disappointed that President Bush' proposed budget for fiscal year 2006 reduces from 0.75 percent to 0.25 percent the all-state minimum formula, which I authored, in applying it to the programs under the State Homeland Security Grant Program. This formula assures that each State receives a minimum of 0.75 percent of those grants to help support their first responders' basic preparedness needs.

Not only would this change result in the loss of millions in homeland security funding for the fire, police and rescue departments in small- and many medium-sized states, but also deal a crippling blow to their efforts to build and sustain their terrorism preparedness.

Mr. Secretary, does this Administration want to shortchange rural states, rolling back the hard-won progress we have begun to make in homeland security by slashing the protections provided to us by the all-state minimum?

Answer. For fiscal year 2006, DHS proposes to redesign the homeland security funding process to award State HSGP funds based on an evaluation of risk and needs. The intent of this approach is to change the way DHS invests its limited homeland security resources in order to achieve the greatest return on investment for our nation's homeland security. This is consistent with recommendations from the 9/11 Commission, which contends that Federal homeland security assistance should supplement State and local resources based on the risks or vulnerabilities that merit additional support. As proposed, fiscal year 2006 awards will be based on a relative evaluation of risk and application-based review of need with no State receiving less than 0.25 percent. DHS will consider risk factors such as threat, presence of critical infrastructure, vulnerability, population and population density, international borders, and ports of entry in making final award determinations. In the consideration of need, DHS will undertake an assessment with the States and territories to identify their capabilities and gaps consistent with the capabilities and tasks identified under Homeland Security Presidential Directive-8. In addition, at least 20 percent of funds awarded will be dedicated to support law enforcement terrorism prevention activities. Overall, this approach will result in the achievement of the highest possible readiness to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and the economy.

Question. Mr. Secretary, would you agree that homeland security is a national responsibility shared by all states, regardless of size?

Answer. Yes, DHS strongly believes that homeland security is not only a Federal responsibility, but it requires collective national and even international action. The protection of our citizens, our critical infrastructure, our businesses, and our communities is a shared responsibility, requiring Federal, state, local, international, and private sector partnerships. The partnership required to protect the homeland involves sharing information as well as responsibility. For that reason, allocation of State and local grant funding should reflect the best available data and analysis of the threats, risks, and unmet needs—not static formulas.

Question. Mr. Secretary, do you agree that each State has basic terrorism preparedness needs and, therefore, a minimum amount of domestic terrorism preparedness funds is appropriate for each state?

Answer. The President's Request proposes a 0.25 percent allocation to be provided to each State as a supplement to State and local resources allocated to domestic preparedness. DHS resources should be used to enhance basic levels of preparedness and not to supplant State and local responsibilities. In addition, the Department believes that States and urban areas should focus on a set of collective capabilities needed to prevent, protect against, respond to, or recover from a terrorist attack or catastrophic event. Through the newly-developed Interim National Preparedness Goal and the accompanying National Planning Scenarios and Target Capabilities List, the Nation will begin to implement a coordinated approach to national preparedness, utilizing a risk-based and regional methodology.

Question. If you do not support applying the 0.75 percent minimum to the State Formula Grants Program, what compromise between 0.75 percent and 0.25 percent for the distribution of funds would you support?

Answer. The DHS proposal to reduce the minimum State allocation from 0.75 percent to 0.25 percent is based on the redesign of the homeland security program to support a risk and need-based approach to funding. Factors such as threat, presence of critical infrastructure, vulnerability, population, borders, and POEs will be used

to make final award determinations. An increase in the base percentage allocation would result in a reduction in resources available for those States with the greatest risk and needs. Therefore, DHS believes that raising the minimum allocation is not conducive to maintaining maximum readiness.

FIRST RESPONDERS (GENERAL)

Question. President Bush often says that he wants to ensure that our State and local first responders receive the resources necessary to do the job the American public expects them to do. I find that hard to believe, though, when I read that he proposes a $455 million overall cut in funds for State Homeland Security Grant Program, Law Enforcement Terrorism Prevention Program, Emergency Management Performance Grants and other programs SLGCP Office that directly benefit police, fire and medical rescue units. The Administration argues this is justified because it does not believe those funds are "targeted" to homeland security capabilities.

I believe, however, that the current Administration has failed to make first responders a high enough priority by consistently underfunding homeland security efforts of every state.

The Hart-Rudman Terrorism Task Force Report argued that our Nation will fall approximately $98.4 billion short of meeting critical emergency responder needs through this decade's end if current funding levels are maintained. Clearly, the domestic preparedness funds available are still not enough to protect from, prepare for and respond to future domestic terrorist attacks anywhere on American soil.

Would you agree, Mr. Secretary, that to be truly protected from, prepared for and able to respond to terrorist attacks we must look to increase the funds to our Nation's State and local first responders, rather than decrease them, as proposed by the President?

Answer. The President's fiscal year 2006 Budget request includes $3.6 billion for SLGCP to continue our strong commitment and support to the nation's emergency prevention and response community. Of this amount, $1.02 billion is for the State HSGP, which has been significantly redesigned to award funds based on risk and need, while aligning with national priorities. An additional $1.02 billion is for the continuance of the UASI, which targets funds to the nation's highest risk urban areas. Further, the President's request provides $600 million for a new TIP Program to supplement state, local, and private sector infrastructure protection efforts based on critical vulnerabilities. The fiscal year 2006 request also includes a strong commitment to our nation's fire service by providing $500 million for the Assistance to Firefighters Grant Program. The request includes $50 million the CCP and $170 million for the EMPG. For continuation of our commitment to training our nation's first responders, the request includes $94.3 million for SLGCP's State and Local Training Program. The request also includes $59 million for the National Exercise Program, which includes support for State and local exercises and for the National Top Officials exercise series. Finally, the request includes $10.6 million for technical assistance initiatives for State and local agencies and $14.3 million for program evaluation and assessments. Between fiscal year 2002 and fiscal year 2004 the SLGCP awarded homeland security grants totaling $6.1 billion. In fiscal year 2005, SLGCP anticipates awarding an additional $3.64 billion in grants. We believe, at this point, that funding provided to our nation's first responders has been sufficient to address their critical needs.

BORDER PATROL

Question. The intelligence reform bill Congress passed and the President signed last December mandated an increase of 2,000 Border Patrol agents in fiscal year 2006, with an increase of 400 agents at the Northern Border. The President's budget for DHS would pay for an increase of slightly more than 200 agents, or about 10 percent of what Congress called for. None of these new agents would be deployed on our Northern Border.

Why does the Administration believe that an increase of about 200 agents is sufficient to secure our borders?

Answer. Following the terrorist attacks of September 11, 2001, the CBP Border Patrol has accelerated its efforts in increasing its enforcement presence along the northern border to achieve the definitive goal of operational control, and the number of agents allowing the northern border more than tripled. DHS is completing work on comprehensive immigration reform, which calls for additional new hires. We have supported additional agents in fiscal year 2006 consistent with both House and Senate appropriation marks for CBP hiring.

Question. Would additional agents beyond the number proposed by the President be useful to the Department's efforts to prevent illegal entry into the United States?

Answer. The Department appreciates the 500 additional agents funded in the Emergency Supplemental. As noted above, the Department is in the midst of a systems-level review of its border control architecture.

ICE/CBP MERGER

Question. As you know, there has been substantial discussion in recent months about a possible merger of Immigration and Customs Enforcement with Customs and Border Patrol. Do you support such a merger?

Answer. I do not support a merger at this time. ICE and CBP were formed just two and a half years ago and the transition to the current structure has been challenging. I am concerned about embarking on yet another far reaching transition affecting these organizations. Most importantly, however, it is too soon to say that the current structure will not effectively serve our border missions. As we move forward with comprehensive reforms and improvement to our border security and immigration system, I am confident that both ICE and CBP can operate in an effectively coordinated manner without being merged.

QUESTIONS SUBMITTED BY SENATOR PATTY MURRAY

PORT SECURITY

Question. Mr. Secretary, one of my greatest concerns—as a Senator from a State that depends on its seaports for its livelihood—is that we have a cohesive port security plan that protects our communities and our economy from potential threats.

Yet the Administration's budget request again seeks to eliminate the Port Security Grant program.

Mr. Secretary, as I've mentioned before, the Coast Guard Commandant testified that it would take more than $7 billion to implement the Maritime Transportation Security Act. To date, we have provided a little more than $500 million toward this $7 billion—most of which was not requested by the Administration. Mr. Secretary, for the past 2 years, nearly $1 billion in port security grant requests came to DHS annually. And, the American Association of Ports Authorities has estimated that there is a need of at least $400 million to help secure our port facilities this year. From our discussions, I know that securing our ports is a priority for you. And, again, I realize you did not draft this budget—but you've been sent here to defend it.

I must ask—is this a budget game the Administration is playing, or does the White House discount all of the intelligence reports that tell us our ports are a significant risk?

Answer. Enhancing the security of the nation's critical infrastructure, especially its ports, continues to remain a high priority for the Department. For fiscal year 2006, DHS is proposing to consolidate the Port Security, Rail/Transit Security, Buffer Zone Protection (BZP) Program and Trucking Industry Security grant programs into the single TIP Program. Combined resources for the fiscal year 2005 distinct programs totaled $315 million. The DHS fiscal year 2006 request for the TIP Program is $600 million, almost double the amount of fiscal year 2005 available resources for the distinct fiscal year 2005 programs. With that being said, funds provided through TIP will directly enhance the ability of the owners and operators of key port assets and transit systems to prevent and respond to large scale incidents. In fiscal year 2005, DHS shifted to a more risk-based allocation of funding across sectors, as well as integration of these programs with regional homeland security planning efforts, such as those required by the UASI. The fiscal year 2005 program also considers intelligence and threat data to set specific security enhancement priorities. The fiscal year 2006 TIP Program will continue to build on these enhancements by shifting to a discretionary approach for all program elements, allowing DHS to better supplement state, local and private sector infrastructure based on risk. Additional priorities for the fiscal year 2006 program include further enhancing the linkages between critical infrastructure protection and regional planning efforts, and a continued emphasis on security investment at ports and transit agencies based on relevant intelligence and threat data. In the end, this will result in a more agile and responsive program based on risk.

CARGO SECURITY

Question. Mr. Secretary, I know we both agree the agencies involved in securing these seaports are doing an admirable job—they are working through a difficult problem.

Yet, they aren't being given the proper tools, resources, and guidance to knit together a coordinated port security regime for our nation.

Last year, I added language into the fiscal year 2005 Committee Report that directed the Under Secretary of Border and Transportation Security to develop a plan to create that coordinated approach to port security. That report was due—quote—no later than February 8, 2005. Yet, we have not received that report. Unfortunately, the message that the Administration has sent is that the White House is not willing to take the responsibility for developing and implementing such a plan.

Mr. Secretary, I've discussed this issue at great length with you, Deputy Secretary Jackson, Commissioner Bonner, your predecessors—anyone who might listen.

I've talked about legislation and additional funding but all we have seen from the Administration is a directive that appointed a new Commission to study the issue.

Mr. Secretary, I know we agree this is an issue of importance. What do you believe we need to do—how can we help you come up with a coordinated approach to secure our ports, the cargo moving through them and the people who work and live near them?

Answer. The report was submitted on June 8, 2005.

Maritime and supply chain security remain priorities for DHS. When the President signed HSPD–13/NSPD 41 in December 2005, he indicated the Administration's commitment to addressing port security as part of the greater maritime system. In this Directive, DHS and DOD were directed by the President to develop a strategy for securing the Maritime domain, including a variety of issues related to port and cargo security. DHS is actively working with DOD and other Federal partners to meet this goal.

In addition, I am reviewing the status of DHS's cargo security efforts, how they can be further strengthened and how we can further transform the system to ensure the United States security and economic needs are met.

HAMMER TRAINING

Question. Mr. Secretary, as you might be aware, Washington State is home to the The Volpentest Hazardous Materials and Emergency Response Training and Education Center—we know it as HAMMER.

This is a state-of-the-art, Department of Energy facility with expertise in threats posed by chemical, radiological, and biological agents, hazardous materials, and weapons of mass destruction. HAMMER specializing in hands-on training for first responders but the Department has not designated this facility a regional training center. Instead, first responders from throughout the Northwest have to use their local budget—or DHS funding—to travel to facilities around the country for the training they could receive close to home. Under the fiscal year 1999 Defense Authorization Act, the Secretary of Energy was specifically authorized to enter into partnership arrangements with to share the facilities at HAMMER with Federal agencies. Under the Homeland Security Act of 2002, you are authorized to enter into joint sponsorship arrangements with the Secretary of Energy to use DOE sites to carry out the missions of the Department of Homeland Security. Mr. Secretary, we have a great facility at HAMMER and I encourage you to come personally, or send your staff out to visit. I know that when you see their capabilities, you will agree that using HAMMER as a designated training center would be a benefit to both the first responder community throughout the Northwest—and DHS itself.

Will you visit HAMMER and consider adding it as a member of the National Domestic Preparedness Consortium?

Answer. The NDPC was chosen based on each member's expertise in first response training. At present, plans to expand DHS' training network are extremely limited, and more than likely will not include the establishment of additional consortium members or residential training facilities. Under the provisions of the Department of Homeland Security's fiscal year 2004 Appropriations Act (Public Law 108–90), ODP received funds for a limited "competitive training grants" program to supplement training efforts provided through the National Domestic Preparedness Consortium. The Competitive Training Grant Program (CTGP) was developed to facilitate national scale training programs, and the fiscal year 2004 program funded 14 training sites. Currently, the Department is undergoing its evaluation process for fiscal year 2005 CTGP applicants. In addition, enhancing existing training programs is an eligible use of other SLGCP grant funds. The Department encourages HAMMER to explore the use of other DHS grants as a potential source of Federal funding in the future.

NORTHERN BORDER SECURITY

Question. Mr. Secretary, the President's budget request only includes funding for 210 of the 2,000 new border agents called for by the Intelligence Reform Act that was signed into law last December.

We currently have about 11,000 Border Patrol agents and 90 percent of them are stationed on the southern border. We have a major security issues at our northern border—ranging from drug trafficking to the apprehension of potential terrorists—and they aren't being addressed.

What kind of message is this sending to our border communities? Is stepping up this security going to be a priority for you?

Answer. Following the terrorist attacks of September 11, 2001, the CBP Border Patrol has accelerated its efforts in increasing its enforcement presence along the Northern Border to achieve the definitive goal of operational control, and the number of agents allowing the Northern Border more than tripled. This accelerated and focused effort has clearly provided the Nation with a more secure Northern Border. Moreover, Emergency Supplemental Legislation and President Bush's fiscal year 2006 Budget call for the hiring of an additional 710 agents by the end of fiscal year 2006, and CBP is taking aggressive steps to recruit, hire and train candidates to fill these spots. The hiring of these new agents comes in addition to the standard attrition hires that supplement the several hundred agents who retire, transfer, or leave for medical reasons over the course of a year. New agent positions will be allocated based on risk-based priorities. That said, effective control of the border—Northern or Southern—requires a more comprehensive approach than simply adding more agents.

DHS is accordingly in the midst of a systems-level review of its border control architecture to identify the right mix of personnel, technology and infrastructure to help achieve effective control of the border. DHS will identify a program manager to oversee the development of a specific set of border security plans.

NORTHERN BORDER AIR WING

Question. Along those lines, the first Customs Air and Marine Operations Wing was established in Bellingham, WA last summer. I was very happy to be there at the dedication and have worked with Director Stallworth to get the program up and running. The second air wing is in Up-State New York and 3 more are planned. We need to make these a priority—especially with the lack of Border Patrol agents on the Northern Border. They also need to be able to communicate with the local law enforcement. Since that time it has become clear that many local law enforcement jurisdictions don't have compatible radios—our eyes-in-the-sky can't coordinate with the police on the ground. I'm told it would cost about $5 million to run a pilot program.

Do you agree that this is an issue we should deal with? Will you help make this happen?

Answer. Deployment of additional Northern Border airwings will be addressed as part of the CBP Air and Marine program integration review now underway. This review is expected to be completed in the summer of fiscal year 2005.

NORTHERN BORDER PROSECUTIONS

Question. Mr. Secretary, because of the increased presence and law enforcement activity on the northern border, incarcerations and prosecutions are up dramatically since September 11. The major border crossing between Seattle and Vancouver, BC is in Blaine—a very small community compared to Detroit and Buffalo—and a very limited local tax base to cover these costs. This community has already seen more than a $3 million increase in prosecution costs simply because they are located on the border. This trend is expected to continue with an expected $4 million in prosecution and incarceration costs in fiscal year 2005. Mr. Secretary, this community needs some special help—they don't have the tax base or population to sustain this and even greater increases.

What can your Department do to help communities like this one?

Answer. DHS has committed significant resources to address the increase in smuggling activity between the United States and Canada, as well as the demonstrated vulnerabilities that exist on the Northern Border. This dedication of enforcement resources has resulted in an increase in arrests, seizures, and prosecutions involving border related criminal activity. Some prosecutions based on DHS enforcement activities have been deferred to the State for prosecution since the violators also fall under State law.

SEATAC AIRPORT

Question. Secretary Chertoff, I am very concerned with the reports that Seattle Tacoma International Airport in Washington State may see a reduction in their Federal security screener force this year. Currently, SeaTac Airport is facing a shortage of approximately 200 FTEs to meet the summer travel season at present staffing levels. Without these additional screeners SeaTac will undoubtedly see repeats of 2002 and 2003 that saw security lines regularly exceeding 1 hour.

Mr. Secretary, I request that you review the situation at SeaTac and work with the local Federal Security Director to ensure that SeaTac's screener staffing level allows the airport and TSA to provide the same level of customer service achieved last year.

Answer. Based on the Screener Staffing Model, SeaTac Airport (SEA) is currently below its required staffing level. TSA is in the process of bringing SEA up to that staffing level. Recruitment of new screeners is underway.

SUBCOMMITTEE RECESS

Senator GREGG. The hearing is recessed.

[Whereupon, at 12:09 p.m., Wednesday, April 20, the subcommittee was recessed, to reconvene to subject to the call of the Chair.]

DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR FISCAL YEAR 2006

THURSDAY, APRIL 28, 2005

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10:29 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Judd Gregg (chairman) presiding.

Present: Senators Gregg, Cochran, Stevens, Craig, Allard, Byrd, and Inouye.

DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF DR. PENROSE C. ALBRIGHT, ASSISTANT SECRETARY FOR SCIENCE AND TECHNOLOGY

OPENING STATEMENT OF SENATOR JUDD GREGG

Senator GREGG. We will convene this hearing.

The purpose of this Homeland Security hearing is to review where we stand relative to defending this Nation from biological or chemical attack, which is in my opinion the biggest threat to our country. If you prioritize threat, which is exactly what we should be doing as a Congress and as a Government, you have to put at the top of the list the concerns weapons of mass destruction used against the American population somewhere here in the United States or overseas obviously.

We, 2 years ago, began the effort to try to aggressively address this issue, recognizing some fundamental flaws within our structure as a country, the biggest flaw being the pharmaceutical industry, which one would presume would naturally pursue ways of being able to respond to a biological attack, was not structured to do so, and the Government was not structured to deal with a chemical or a biological attack.

BIOSHIELD

So we worked very hard, in my prior role as Chairman of the Health Committee, to pass a piece of legislation called BioShield, which was the initiative of the administration. And the purpose of this bill was to reenergize the vaccine industry in this country and to energize the research community within our Nation to pursue ways to respond to various chemical and biological agents which might be used against us.

We understand, obviously, there is no market for a product to respond to these type of agents. These agents are by definition agents

which do not commonly occur, but only occur when we are attacked, although smallpox was a problem, but it has been eradicated. So we needed to create a structure where there would be not only an atmosphere where creative individuals and scientists would step forward to develop responses to attacks involving threats such as anthrax, smallpox, botulism, and plague, but we also had to create a monetary system, a market system which would encourage this from a standpoint of making it a reasonable place to invest your money if you were an investor. And that is what BioShield was all about. It basically put the Government in the business of buying antidotes and vaccines for this list of major threats.

We are now well into this process. Progress has been made in some areas but there is still a long way to go in other areas. The purpose of this hearing is to discuss what we are doing and what we should be doing that will better produce results.

My own personal concern is we have still not stood up a vaccine industry in this country at the level I would like to see it. We still do not have many participants in the production of vaccine, that the research community, especially our academic research community, has not yet embraced this initiative as well as and as aggressively as I would hope, and that there appears to be some incentives in the system which are discouraging research in this area, and the question of how we are purchasing products, to the extent it is being brought on line, whether that is chilling competition or participation of other parties in the research and development of creative new ways to address these types of threats.

It is a complex issue involving the most cutting-edge levels of science, and it does not have a simple solution. If it did, we would have gotten to it much sooner. But we do have a committed effort to do it, and we have got a committed Government to accomplish it, and I think we have got some good witnesses today to find out where we stand and where we should go.

With that, I will yield to the honorable Senator from Virginia, Senator Byrd.

STATEMENT OF SENATOR ROBERT C. BYRD

Senator BYRD. That is West Virginia.

Senator GREGG. I apologize profusely.

BIOLOGICAL OR CHEMICAL ATTACK

Senator BYRD. Mr. Chairman, first of all, let me thank you for your service. I listened with rapt attention at your remarks. You are well prepared to be the Chairman of this subcommittee and well prepared to probe this very important subject.

I welcome the witnesses on both panels for this hearing, and I applaud you, Mr. Chairman, for calling us together for such an important topic.

Earlier this year during testimony before the Senate Intelligence Committee, CIA Director Porter Goss warned and I quote "It is only a matter of time before Al Qaeda or another terrorist group tries to use chemical, biological, radiological, or nuclear weapons in the United States." Mr. Chairman, I believe that. I believe it is absolutely the case, and I am not sure that we are prepared. I doubt it because we do not know when, we do not know where this mon-

ster will confront us with a bioterror attack, a chemical attack, a nuclear attack, or a radiological attack.

With regard to a biological attack, Congress made a serious commitment by appropriating $5.6 billion to pursue new vaccines and medications to protect the American public from known biological threats. It is essential the agencies involved in this process be accountable for progress in this area. So, I look forward to discussing this and other homeland security efforts, not only to detect and respond to a bioterror incident, but what efforts are being made to prevent a biological, chemical, also to examine nuclear terror incident.

Thank you, Mr. Chairman.

Senator GREGG. Thank you, Senator Byrd.

We will turn to the panel now. The first panel will be people in our Government who have first-line responsibility for getting us prepared for a biological or chemical attack and being able to respond to it. Our first witness is Dr. Albright who was confirmed as Assistant Secretary of Homeland Security, Plans, Programs, and Budgets on October 3. Our second witness is Mr. Simonson who is the Assistant Secretary for Public Health Emergency Preparedness, United States Department of Health and Human Services. And these two gentlemen have the portfolio and we look forward to hearing how we are doing. So let us start with you, Dr. Albright.

STATEMENT OF DR. PENROSE C. ALBRIGHT

Dr. ALBRIGHT. Good afternoon, Chairman Gregg, Senator Byrd, and distinguished members of the Subcommittee. I am pleased to appear before you today to discuss the progress the Science and Technology Directorate of the Department of Homeland Security is making in the Nation's efforts to prevent, protect against, respond to, and recover from acts of bioterrorism against the American people.

President Bush has made strengthening the Nation's defenses against biological weapons a critical national priority. The President's focus on these issues has resulted in a joint Homeland Security Presidential Directive/National Security Presidential directive entitled Biodefense for the 21st Century that provides a comprehensive framework for our Nation's sustained and focused effort against biological weapons threats.

ACCOMPLISHMENTS IN BIODEFENSE

The Department of Homeland Security and the Science and Technology Directorate have explicit responsibilities in this integrated national effort. In particular, I want to highlight the strategy, planning, and accomplishments to date of the Science and Technology Directorate in the area of biodefense and the essential collaborations with key Federal partners, including those represented here today.

In 2004 and 2005, the Science and Technology Directorate developed a national architecture and plan for the detection of biological attacks, should they occur, and as initial steps, deployed the BioWatch Environmental Sensor System to protect our Nation's cities from the threat and ramifications of such an attack and also

initiated the design of the National Biosurveillance Integration System as part of an interagency process.

We completed the planning and conceptual design of the National Biodefense Analysis and Countermeasures Center. This center will focus on, among other things, creating a scientifically based understanding of the biological threat.

We established the Biodefense Knowledge Center, which is an operational hub for enabling collaboration and communication within the Homeland Security enterprise. We have certified four material threats and have two additional certifications underway. These material threat determinations are required in order to commit BioShield funds.

We have established a National Bioforensic Analysis Center to provide a national capability for conducting forensic analysis of evidence from biocrimes and terrorism to obtain a biological fingerprint to identify perpetrators and determine the origin and method of the attack.

In 2006, our expectations are to complete the deployment of the second generation BioWatch system to the top threat cities and to complete test and evaluation of the laboratory prototypes for the third generation of these detection systems.

We will also complete the first formal risk assessment that is required under HSPD-10 and close many of the key remaining experimental gaps in our knowledge of the classic biological threat agents.

We will continue operations of the Plum Island Animal Disease Center and essential upgrades to the facility and initiate the design of the National Bio and Agrodefense Facility.

We continue to develop bioassays for Foot and Mouth Disease and look-alike animal diseases. We continue to conduct cutting-edge research in academia through our Homeland Security Centers of Excellence. Although each of the four centers we have has a role in addressing bioterrorism, let me highlight two.

One is at Texas A&M and its partners which study foreign animal and zoonotic diseases at the National Center for Foreign Animal and Zoonotic Disease, and they address potential threats to animal agriculture, including Foot and Mouth Disease, Rift Valley fever, Avian influenza, Brucellosis, that sort of thing.

The University of Minnesota and its partners established best practices and attract new researchers to manage and respond to food contamination events.

S&T DIRECTORATE'S INTERAGENCY COLLABORATION

Ensuring that all relevant Federal Departments and agencies coordinate in the area of biodefense is critical to protecting the Nation from biological threats. The Science and Technology Directorate has been and continues to be an active participant in relevant interagency activities. A full list of the S&T Directorate's interagency collaborations is in my statement for the record. Highlights include our integral participation in the creation of HSPD–10. We also participate in the Counterproliferation Technology Coordinating Committee, the National Science and Technology Council's Weapons of Mass Destruction Medical Countermeasures Committee, which is really crucial to our way ahead on BioShield. This

last, which I personally co-chair, provides an interagency forum for discussing and prioritizing the medical countermeasure needs, as I said, that will be pursued under the BioShield program.

We work closely with our colleagues in the Department of Health and Human Services and USDA. Mr. Simonson and I see each other very frequently, and he and I and our staffs interact nearly daily in our respective efforts to protect the Nation from the threats of bioterrorism.

As I hope I have indicated, the Science and Technology Directorate's programs fully support the National Biodefense Program, as stated in HSPD–10. Moreover, they are conducted in an active collaboration with other Federal Departments and agencies, having a role in meeting this national priority and are focused on reducing the threat of a biological attack against the Nation's population and its agricultural and food infrastructures. We also support a science-based forensics and attribution capability.

PREPARED STATEMENT

This concludes my prepared statement. With the subcommittee's permission, I request that my formal statement be submitted for the record. Mr. Chairman, Senator Byrd, members of the subcommittee, I thank you for the opportunity to appear before you and will be happy to answer any questions that you may have.

[The statement follows:]

PREPARED STATEMENT OF DR. PENROSE C. ALBRIGHT

INTRODUCTION

Good afternoon, Chairman Gregg, Senator Byrd and distinguished members of the Subcommittee. I am pleased to appear before you today to discuss the progress the Science and Technology Directorate of the Department of Homeland Security is making in the Nation's efforts to prevent, protect against, respond to, and recover from acts of bioterrorism against the American people.

President Bush has made strengthening the Nation's defenses against biological weapons a critical national priority. Although significant progress has been made to protect America, President Bush instructed Federal departments and agencies to review their efforts and find better ways to secure America from bioattacks.

This review resulted in a Presidential Directive entitled Biodefense for the 21st Century that provides a comprehensive framework for our Nation's biodefense. This directive builds upon past accomplishments, defines specifies roles and responsibilities, and integrates the programs and efforts of various communities: national security, medical, public health, intelligence, diplomatic, agricultural and law enforcement into a sustained and focused effort against biological weapons threats.

The Department of Homeland Security (DHS) and the Science and Technology (S&T) Directorate have explicit responsibilities in this integrated national effort. In particular, I want to highlight the strategy, planning and accomplishments to date of the Science and Technology Directorate in the area of biodefense, and the essential collaborations with key Federal partners.

BIODEFENSE

Before I speak directly to the biodefense efforts of the S&T Directorate, I want to briefly address the role of the DHS's Information Analysis and Infrastructure Protection Directorate (IAIP), and how their work is linked to the S&T Directorate. IAIP assesses intelligence and information about threats and vulnerabilities from other agencies and takes preventative and protective action. They are partners in the total interagency efforts to obtain, assess and disseminate information regarding potential threats to America from terrorist actions. These threat and vulnerability assessments are inputs into the strategy and research, development, testing and evaluation (RDT&E) activities of the Science and Technology Directorate. For example, agriculture and food are two of the multiple critical infrastructure sectors iden-

tified by Homeland Security Presidential Directive 7 (HSPD–7). As such, they fall within the domain of the IAIP Directorate; they are also within the domain of concern for biological threats and are considered in HSPD–9 and HSPD–10/National Security Presidential Directive-33 (NSPD–33). In addition, the IAIP Directorate's cooperation with the Science and Technology Directorate is critical to the Department's mission to determine what agents would significantly impact national security if released (Material Threat Determinations).

Mission and Objectives

HSPD–10 outlines four essential pillars of the Nation's biodefense program and provides specific directives to further strengthen the significant gains made in the past 3 years. The four pillars of the program are:

—*Threat Awareness.*—Which includes biological weapons-related intelligence, vulnerability assessments, and anticipation of future threats. New initiatives will improve our ability to collect, analyze, and disseminate intelligence on biological weapons and their potential users.

—*Prevention and Protection.*—Which includes interdiction and critical infrastructure protection. New initiatives will improve our ability to detect, interdict, and seize weapons technologies and materials to disrupt the proliferation trade, and to pursue proliferators through strengthened law enforcement cooperation.

—*Surveillance and Detection.*—Which includes attack warning and attribution. New initiatives will further strengthen the biosurveillance capabilities being put in place in fiscal year 2005.

—*Response and Recovery.*—Which includes response planning, mass casualty care, risk communication, medical countermeasures, and decontamination. New initiatives will strengthen our ability to provide mass casualty care and to decontaminate the site of an attack.

The Department of Homeland Security has a role and responsibility in each of these four pillars of the national biodefense program. The S&T Directorate has the responsibility to lead the Department's RDT&E activities to support the national biodefense objectives and the Department's mission.

Accomplishments and Planned Activities

In fiscal year 2004 and fiscal year 2005, the Biological Countermeasures portfolio:

—Deployed the BioWatch environmental sensor system to protect our Nation's cities from the threat and ramifications of a bioterrorist attack.

—Engaged in creating additional near real-time monitoring (Autonomous Pathogen Detection System) of critical infrastructure facilities such as major transportation hubs. New infrastructure protection efforts include shorter response time biological agent detection capabilities for BioWatch. This pilot (second generation Bio Watch) is in the process of being deployed in New York City and will join an expansion of the number of collectors in that city.

—Initiated the design of the National Biosurveillance Integration System (NBIS) as part of an interagency process. Recently completed in the first quarter of fiscal year 2005, we will work with the Information Analysis and Infrastructure Protection (IAIP) Directorate to implement this system.

—Conducted preliminary analyses, using the reference scenario approach recommended by Homeland Security Presidential Directive (HSPD)–10 for understanding the requirements of an integrated national biodefense architecture, of four baseline reference cases: a large outdoor release of a non-contagious agent (anthrax); a large indoor release of a contagious agent (smallpox); contamination of a bulk food supply; and two highly virulent agricultural attacks, one on livestock (Foot and Mouth Disease) and the other on crops (soy bean rust).

—Established the Biodefense Knowledge Center, an operational hub for enabling collaboration and communication within the homeland security complex. The Biodefense Knowledge Center will meet the operational and planning requirements of government decision-makers and program planners, the intelligence community, law enforcement officers, public health practitioners, and scientists. Specific capabilities offered to these end-users include knowledge services, modeling and simulation, situational awareness and a pathway to accelerate research and development.

—Certified four "material threats" (anthrax, smallpox, botulinum toxin, and radiological/nuclear); will complete the rest of the Category A bioagents (plague, tularemia) by the end of fiscal year 2005.

—Established the National Bioforensic Analysis Center (NBFAC) to provide a national capability for conducting forensic analyses of evidence from bio-crimes and terrorism to attain a "biological fingerprint" to identify perpetrators and determine the origin and method of attack. The NBFAC was named in HSPD–

10 as the lead Federal facility to conduct and facilitate the technical forensic analysis of materials recovered following a biological attack in support of the appropriate lead Federal agency [in most cases the lead Federal agency will be the Federal Bureau of Investigation (FBI)].

In fiscal year 2006, the Biological Countermeasure portfolio plans to:

—Complete the three high-level architectures initiated in fiscal year 2005, identifying key requirements for each major element, a "report card" on the current and projected status in that area and performing detailed design tradeoffs for those areas in which DHS has execution responsibility.

—Complete the first formal risk assessment required under HSPD–10 and close many of the key remaining experimental gaps in our knowledge of the classical biological threat agents. Near-, mid-, and long-term plans for dealing with engineered agents will be developed, and R&D on addressing the gaps in responding to genetically modified organisms (e.g., antibiotic resistant) initiated.

—Complete the deployment of Generation 2 BioWatch systems to additional cities while continuing to operate and optimize already extant BioWatch systems.

—Complete test and evaluation of laboratory prototypes of the Generation 3 BioWatch detection systems for selection of fieldable prototypes for fiscal year 2007.

—Continue operation of the interim National Bioforensic Analysis Center. International Organization for Standardization (ISO) certification is expected to

—5 have been achieved, giving the analyses conducted additional credibility and authenticity in both the national and international community and courts of law. R&D will continue on the physical and chemical signatures of the "matrix" materials associated with biological agents so as to develop methods for understanding tell-tale remnants of enrichment media, culture conditions, metabolites, and dispersion technology.

—Continue operation of the Plum Island Animal Disease Center (PIADC) and essential upgrades to the facility and initiate design of the National Bio and Agrodefense Facility (NBAF). R&D will continue on next generation vaccines and antiviral therapeutics for foot and mouth disease (FMD) and other high priority foreign animal diseases.

—Continue to develop bioassays for FMD and look-alike animal diseases. The initial agricultural forensic capability established in fiscal year 2004 at PIADC will be enhanced and epidemiologic capability added. A High Throughput Diagnostics Demonstration will be initiated to work with regional and State laboratories to demonstrate a capability of analyzing thousands of samples per day in support of response to a suspected case or an outbreak. A FMD table top exercise will be conducted, and development of a coupled epidemiological and economic model for FMD will begin. The end-to-end systems study initiated in fiscal year 2004 for Soybean Rust and FMD will be completed, and system studies will be initiated for highly pathogenic avian influenza.

National Bio-Defense Analysis and Countermeasures Center (NBACC)

The NBACC, a key component of the National Strategy for Homeland Security, addresses the need for scientific research to better anticipate, prevent, and mitigate the consequences of biological attacks. The need for the NBACC facility is further defined in HSPD–10, the Nation's blueprint for future biodefense programs. The NBACC's mission will support two pillars of this blueprint—threat awareness and surveillance and detection. The NBACC is made up of two centers, the Biological Threat Characterization Center and the National Bioforensic Analysis Center to carry out these missions. Specifically, NBACC's mission is to:

—Understand current and future biological threats, assess vulnerabilities, and determine potential impacts to guide the research, development, and acquisition of biodefense countermeasures such as detectors, drugs, vaccines and decontamination technologies; and

—Provide a national capability for conducting forensic analysis of evidence from bio-crimes and terrorism to attain a "biological fingerprint" to identify perpetrators and determine the origin and method of attack.

In fiscal year 2004, the Department completed the planning and conceptual design of the NBACC facility. Additionally, the Department has been working through the National Environmental Policy Act (NEPA) process during the year, which culminated in the signing of the Record of Decision in January 2005 of the Final Environmental Impact Statement (EIS) for the construction project and subsequent operations. It was decided to delay the award of any contracts for design and construction until further in the EIS process. As the public concerns are analyzed and considered it is anticipated that contracts will be awarded in fiscal year 2005 to initiate design and construction of the NBACC facility

In fiscal year 2005, the solicitations of contracts for the construction of the NBACC facility are expected to be awarded. The design of the NBACC facility will commence in March 2005. Congress appropriated $128 million in obligated funds, of which $35 million was appropriated for award of the construction contract in the fourth quarter of fiscal year 2005. Construction of the facility is planned for completion by the fourth quarter of fiscal year 2008.

University Centers of Excellence

The mission of the University Programs is to stimulate, coordinate, leverage and utilize the unique intellectual capital in the academic community to address current and future homeland security challenges, and to educate and inspire the next generation of scientists and engineers dedicated to homeland security.

Within the University Programs in the S&T Directorate, the Homeland Security (HS) Centers of Excellence provide independent, cutting-edge research in academia for focused areas of homeland security Research and Development. Established centers include: the Homeland Security Center for Risk and Economic Analysis of Terrorism Events, the National Center for Foreign Animal Disease and Zoonotic Defense, and the National Center for Food Protection and Defense. In the next few months, the S&T Directorate expects to establish the Homeland Security Center for Behavioral and Social Aspects of Terrorism and Counter-Terrorism. Each Center is selected on a competitive basis, and each grant is for 3 years. Each Center has a role in addressing bioterrorism and two are specifically aligned with addressing bioterrorism.

DHS awarded funds, over 3 years, to the University of Southern California (USC) and its major partners, University of Wisconsin at Madison, New York University and Structured Decisions Corporation (affiliated with MIT) to establish the Center on Risk and Economic Analysis of Terrorism Events. The mission objectives are to evaluate the risks, costs and consequences of terrorism and to guide economically viable investments in countermeasures. Specifically, the Center will develop risk assessment and economic modeling capabilities that cut across general threats and targets, in application areas such as electrical power, transportation and telecommunications. Additionally, USC and their partners will develop tools for planning responses to emergencies, to minimize the threat to human life and reduce economic impacts of terrorist attacks.

Texas A&M University and its partners from the University of Texas Medical Branch, University of California at Davis, and the University of Southern California expect to receive funds over the course of the next 3 years for the study of foreign animal and zoonotic diseases. The Center, which will be known as the National Center for Foreign Animal and Zoonotic Disease Defense, will work closely with partners in academia, industry and government to address potential threats to animal agriculture including Foot and Mouth Disease, Rift Valley fever, Avian influenza and Brucellosis. The Foot and Mouth Disease research will be conducted in close collaboration with DHS's Plum Island Animal Disease Center.

The Department of Homeland Security will provide the University of Minnesota and its partners, Michigan State University, University of Wisconsin at Madison, North Dakota State University, Georgia Institute of Technology, and the University of Tennessee at Knoxville with funds over the course of the next 3 years to establish best practices and attract new researchers to manage and respond to food contamination events, both intentional and naturally occurring. The University of Minnesota's National Center for Food Protection and Defense, will address agricultural security issues related to postharvest food protection.

Negotiations began January 10, 2005, for a 3-year grant with the University of Maryland for a fourth Center on Behavioral and Social Research on Terrorism and Counter-Terrorism. We expect its mission objectives to be to provide strategies for intervention of terrorists and terrorist organizations and to embolden the resilience of U.S. citizens. Major domestic partners include, the University of California at Los Angeles, University of Colorado, Monterey Institute of International Studies, University of Pennsylvania, and the University of South Carolina.

A broad agency announcement was released in mid-January, 2005 for proposals for a fifth DHS Center of Excellence on the topic of High Consequence Event Preparedness and Response.

In addition to the University Centers of Excellence, the Department of Homeland Security's University Programs and the Environmental Protection Agency's Science to Achieve Results (STAR) Program are reviewing proposals for a research Center of Excellence focused on an area of high priority to both Agencies, Microbial Risk Assessment (MRA) for Category A bio-threat agents.

Interagency Collaboration

Ensuring that all relevant Federal Departments and agencies coordinate in the area of Biodefense is critical to protecting the Nation from biological threats. The previously mentioned HSPD–10, as well as other directives including HSPD–9, Defense of United States Agriculture and Food; HSPD–8, National Preparedness; HSPD–4, National Strategy to Combat Weapons of Mass Destruction; and HSPD–7, Critical Infrastructure Identification, Prioritization, and Protection, identify national objectives and priorities, and departmental and agencies' roles in addressing these national objectives.

The S&T Directorate has been, and continues to be an active participant in these interagency activities as illustrated by our participation in the biodefense program. At the highest level HSPD–10/NSPD–33 laid out the overall strategy, department and agency roles, as well as specific objectives and called for periodic reviews to plan, monitor and revise implementation. This was followed by an interagency review, of specific fiscal year 2006-fiscal year 2010 science and technology needs to support the national biodefense strategy as articulated in HSPD–10.

The National Science and Technology Council's Weapons of Mass Destruction Medical Countermeasures Subcommittee (WMD–MCM), co-chaired by the Assistant Secretary of the S&T Directorate, provides an interagency forum for discussing and prioritizing medical countermeasure needs to be pursued under BioShield. At still the next level of coordination, there are strong bilateral efforts around key elements of the strategy. Examples of this coordination including strong and frequent collaborations on Bioshield (HHS/DHS), the development of coordinated civilian and military surveillance and detection systems (DHS/DOD), the development and execution of a National Strategy for Agricultural Biosecurity (DHS/USDA), and development and assessment of decontamination technologies (DHS/EPA).

In addressing these activities, DHS has a leadership role in several key areas and partners with lead agencies in others. Those areas in which the S&T Directorate provides significant leadership are:

—Providing an overall end-to-end understanding of an integrated biodefense strategy, so as to guide the Secretary and the rest of the Department in its responsibility to coordinate the Nation's efforts to deter, detect, and respond to biological acts of terrorism.

—Providing scientific support to the intelligence community and the IAIP Directorate in prioritizing the bio-threats.

—Developing early warning and detection systems to permit timely response to mitigate the consequence of a biological attack.

—Conducting technical forensics to analyze and interpret materials recovered from an attack to support attribution.

—Operation of the Plum Island Animal Disease Center to support both research and development (R&D) and operational response to foreign animal diseases such as foot and mouth disease.

DHS also supports our partnering departments and agencies with their leads in other key areas of an integrated biodefense: the Department of Health and Human Services (HHS) on medical countermeasures and mass casualty response; the U.S. Department of Agriculture (USDA) on agriculture biosecurity; USDA and HHS on food security and the Environmental Protection Agency (EPA) on decontamination and on water security.

In addition, the Science and Technology Directorate has engaged with other Federal Agencies in the following efforts:

—The S&T Directorate worked with DOS (STAS), USDA, Office of Science and Technology Police (OSTP), National Science Foundation (NSF) to create and support the U.S.-Japan Safe and Secure Society forum.

—The Directorate and DOS (OES) jointly created and negotiated the US–UK S&T Memorandum of Agreement (MOA). The resulting MOA supports collaboration on Homeland Security research, development, testing, and evaluation between the United States and the UK.

—The S&T Directorate represents DHS as the lead U.S. agency for the US–CA Public Security Technical Program (PSTP) which is the primary cooperative arrangement on S&T for homeland security between the two countries. Other U.S. agencies involved in the PSTP include: FBI, DOE, DOD, USDA, HHS, DOC (NIST), EPA, DOS, NSA and other DHS components.

—Currently leads a partnership with the Center for Disease Control (CDC), EPA, and FBI on the deployment of BioWatch, a bioaerosol detection system deployed to many of this Nation's cities.

—Funds BioNet—Defense Threat Reduction Agency (DTRA) executed pilot program to integrate civilian and military domestic biodetection and consequence management, using San Diego as a pilot city.

—Leading an interagency effort with HHS, DOD, and the United States Postal Service (USPS) to develop a National Integrated Biomonitoring System, part of HSPD–10 responsibility.
—Primary participant in the establishment of the National Interagency Biodefense Campus being developed at Ft. Detrick.
—The National Bioforensics Analysis Center (NBFAC) is a joint Science and Technology Directorate-FBI program
—In a joint effort with USDA, have developed an integrated national agrodefense strategy, with especial emphasis on foreign animal disease. The Directorate and USDA also conduct joint research and development programs at the Plum Island Animal Disease Center

Presidential Initiatives

Three Presidential Initiatives address the needs of an integrated biodefense strategy and DHS plays a key role in each one. These three initiatives are:

BioShield.—Signed into law July 21, 2004, BioShield is a program coordinated by the Secretary for Homeland Security and the Secretary for Health and Human Services that provides $5.6 billion over 10 years for the purchase and development of countermeasures to WMD. DHS's S&T Directorate plays a significant role in this in determining which agents constitute "material threats" and in developing scenarios that inform decisions on the quantity of countermeasures required. We have certified four "material threats" (anthrax, smallpox, botulinum toxin, radiological/nuclear, and nerve agents), have two additional underway, (plague and tularemia), and the rest of the Category A bioagents should be completed by fiscal year 2006.

Biosurveillance Initiative.—A program that seeks to enhance systems that monitor the Nation's health (human, animal and plant) and its environment (air, food, water) and to integrate these with intelligence data to provide early detection of an attack and the situational understanding needed to guide an effective response. The S&T Directorate plays a major role in the Biosurveillance Initiative in operating its 1st Generation BioWatch System, in deploying a 2nd Generation system and significantly expanding the number of collectors in the highest threat cities and at key facilities (e.g. transportation systems), and in continuing to develop advanced detection systems to further increase the capabilities. We are also designing the information system that will be used to integrate health and environmental monitoring information from the sector specific agencies with intelligence data from the IAIP Directorate. Implementation of this system will actually be initiated by the IAIP Directorate in fiscal year 2005, but the S&T Directorate will continue to supply subject matter expertise in biological threat and defense.

Food and Agricultural Initiative.—Seeks to enhance the security of our agricultural and food infrastructures. DHS activities in this area are led by the IAIP Directorate—but the S&T Directorate brings significant contributions in end-to-end studies of key agricultural and food threats, through the development of advanced diagnostics, and through R&D conducted jointly with USDA at the Plum Island Animal Disease Center.

CONCLUSION

The Science and Technology Directorate's programs conducted within the Department of Homeland Security fully support the national biodefense program as stated in the presidential directive Biodefense for the 21st Century, and other Homeland Security Presidential Directives. Moreover, they are conducted in an active collaboration with other Federal departments and agencies having a role in meeting this national priority, and are focused on reducing the threat of a biological attack against this Nation's population and its agriculture and food critical agricultural infrastructures, and supports a science-based forensics and attribution capability.

This concludes my prepared statement. With the Committee's permission, I request my formal statement be submitted for the record. Mr. Chairman, Senator Byrd, and Members of the Subcommittee, I thank you for the opportunity to appear before you and I will be happy to answer any questions that you may have.

Senator GREGG. Thank you, Mr. Albright.

Before we turn to Mr. Simonson, it is the tradition of this subcommittee to recognize the Chairman of the full committee, whenever he arrives, for any statement he wishes to make.

STATEMENT OF SENATOR THAD COCHRAN

Senator COCHRAN. Mr. Chairman, thank you. Let me congratulate you on the success of the legislation which you authored here in the Senate to establish the legal authority to appropriate funds to deal with threats to our food supply and our agriculture infrastructure and our other concerns in the whole general area of bioterrorism. There is nothing more frightening to contemplate than an attack against these resources and assets in our country, and we do have a serious lack of products, drugs, countermeasures to deal with a serious assault on our food supply and our agriculture infrastructure. So it is very appropriate, I think, that you chair this subcommittee now that is in charge of funding the law you helped create and took a leadership role in, and we appreciate those efforts very much.

I am glad to be here with Dr. Albright and Mr. Simonson to congratulate them on their initiatives and hard work in developing a response structure at the Federal level and to provide national leadership in this very important undertaking.

Thank you.

Senator GREGG. Thank you, Mr. Chairman. I would simply note, it is only through your generosity that I chair this subcommittee, and I am very appreciative of that.

Mr. Simonson.

STATEMENT OF STEWART SIMONSON, J.D., ASSISTANT SECRETARY, OFFICE OF PUBLIC HEALTH EMERGENCY PREPAREDNESS, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. SIMONSON. Good morning, Mr. Chairman, Senator Byrd, Senator Allard, and Senator Craig, and other members of the subcommittee. I am Stewart Simonson, Assistant HHS Secretary for Public Health Emergency Preparedness, and I appreciate the opportunity to share with you information on the progress of implementing the Project BioShield Act of 2004, which was enacted some 9 months ago.

The events of September and October of 2001 made it very clear bioterrorism is a serious threat to our Nation and the world. The Bush administration and Congress responded forcefully to this threat by seeking to strengthen our medical and public health capacities to protect our citizens from future attacks. To encourage the development of new medical countermeasures against threats and to speed their delivery, President Bush in his 2003 State of the Union address proposed and Congress subsequently enacted Project BioShield. The $5.6 billion 10-year special reserve fund was created to assure developers of medical countermeasures that funds would be available to enable the Government to purchase critical products.

Since enactment, my office has moved aggressively to fill immediate gaps in our reserve of medical countermeasures. A sense of urgency has pervaded our efforts and has defined new ways of doing business. Let me briefly describe to you what we have done to address these gaps beginning with anthrax.

ANTHRAX

Anthrax is a serious public health threat, and although the Strategic National Stockpile contains antibiotics sufficient to treat millions of persons exposed to anthrax, the vaccine has an important place in our preparedness and response strategy. The U.S. Government, relying on interagency expert input, defined the initial vaccine requirement for protecting 25 million persons.

The Institute of Medicine, in a report issued in 2002, urged that a new anthrax vaccine based on modern principles of vaccinology be developed. An assessment of developing technologies was undertaken by HHS, experts in the field, and it was determined there was sufficient scientific basis to support the aggressive development of a new generation of vaccine consisting of recombinant protective antigen, the so-called rPA vaccine. Research spanning more than a decade, conducted in large part by the U.S. Government, permitted us to move the vaccine further along the development pipeline. The National Institutes of Health took the lead in working with the private sector to advance development of this new vaccine.

When HHS felt the technology was mature enough to indicate that the vaccine could be licensed within 8 years, my office launched an initiative to acquire it for the Strategic National Stockpile. Utilizing a stringent evaluation process, we reviewed multiple proposals and finally negotiated a contract with VaxGen of Brisbane, California for 75 million doses of vaccine, anticipating a three-dose regimen. The milestone contract with VaxGen lays out an ambitious program, including delivery of the first 25 million doses of usable vaccine within 2 years of award.

I want to draw your attention to a feature of the contract with VaxGen and, indeed, all BioShield contracts. No payment for vaccine is made until the product is received into the stockpile.

To provide for the stockpile's immediate needs, my office is in the process of completing negotiations for 5 million doses of the currently licensed vaccine and hopefully with an option for an additional 5 million doses. We expect those negotiations to be concluded shortly.

But we are focused on threats beyond anthrax as well. My office has moved quickly to address the need for pediatric liquid formulation of potassium iodide, a drug that protects the thyroid from radioactive iodine. This formulation is aimed at young children who are at the greatest risk from the harmful effects of exposure to radioactive iodine. In March, a contract was awarded under Project BioShield for suspension potassium iodide to protect at least 1.7 million children. Product delivery will begin next month.

In addition to the BioShield contracts that have already been awarded, there are several other BioShield procurement related activities underway. We are reviewing the responses for request for proposals for anthrax therapies and we are continuing to move forward on the acquisition of an antitoxin treatment for botulinum.

To signal our intent to acquire a next generation smallpox vaccine, we will be releasing a draft request for proposal for industry comment within the next few weeks.

Finally, in anticipation of yet-to-be-determined requirements, we actively monitor the state of the medical countermeasure pipeline, both within and outside of the U.S. Government, by evaluating Government research and development portfolios and engaging industry to the publication of requests for information. For example, we have released three RFIs to assess the time line to maturity of medical countermeasures to treat nerve agent exposure, acute radiation syndrome, and additional products that might be available to treat anthrax. These requests are key for HHS to dialogue with industry partners to inform them on the development of a sound acquisition strategy.

Defining priorities and quantifying the size of the threat to the population are key steps in focusing our efforts. In the process, we must be mindful of the realities of the spectrum of efforts needed along the research and development pipeline to produce a usable medical countermeasure. The process of defining required specifications for countermeasures often reveals few, if any, candidates in the pipeline. We have been fortunate that some of our highest priority needs for countermeasures could be addressed using the available advanced development products already in the pipeline. However, basic research and early development efforts, when even robustly funded, often take years before a concept is mature enough for advanced development, and it is only when a product has reached the advanced development stage that Project BioShield provides a meaningful incentive for manufacturers to take the product the rest of the way.

PREPARED STATEMENT

In closing, HHS has a clear mandate from President Bush and Congress to lead the charge in countermeasure development. We have already made important strides to address the public health needs of the Nation, but there is more that needs to be done. Mr. Chairman, I look forward to working with you and Senator Byrd and other members of the committee to address the challenges of bioterrorism and to improve the public health of the Nation.

Thank you.

[The statement follows:]

PREPARED STATEMENT OF STEWART SIMONSON

Good morning, Mr. Chairman, Senator Byrd and Subcommittee members. I am Stewart Simonson, Assistant Secretary for Public Health Emergency Preparedness. I appreciate the opportunity to share with you information on our progress in implementing the Project BioShield Act of 2004, which was enacted some 9 months ago. Biodefense is a top priority for the Bush Administration and having an appropriate armamentarium of medical countermeasures is a critical aspect of the response and recovery component of the President's "21st Century Strategy for Biodefense." The acquisition and ready availability of medical countermeasures, such as antibiotics, monoclonal and polyclonal antibodies against infectious threats, therapies for chemical and radiation-induced diseases, and vaccines to protect against exposure from biological agents will have a substantial impact on our preparedness and response capabilities.

PROTECTING AMERICANS

The events of September and October 2001 made it very clear that terrorism—indeed bioterrorism—is a serious threat to our Nation and the world. The Bush Administration and Congress responded forcefully to this threat by seeking to strengthen our medical and public health capacities to protect our citizens from fu-

ture attacks. The Bioterrorism Act of 2002 substantially increased funding authorization for the Centers for Disease Control and Prevention's Strategic National Stockpile. To encourage the development of new medical countermeasures against biological, chemical, or radiological agents and to speed their delivery and use in the time of an attack, President Bush, in his 2003 State of the Union address proposed and Congress subsequently enacted the Project BioShield Act of 2004. The Special Reserve Fund, pre-appropriated with $5.6 billion was created to assure developers of medical countermeasures that funds would be available to purchase critical products for use to protect our citizens.

THE STRATEGIC NATIONAL STOCKPILE TODAY

The wake-up call that we received in the fall of 2001 brought clarity to the gaps in our chemical countermeasure armamentarium and we immediately sought to address them. Although there is much work still to be done, we have made significant progress in building our Strategic National Stockpile from that time to what we have on-hand today. For example, our smallpox vaccine stockpile has grown from 90,000 ready-to-use doses in 2001 to enough vaccine to protect every man, woman, and child in America. Major strides have been made in building our chemical countermeasure reserve against anthrax, plague, and tularemia. We are now able to protect and treat millions of Americans in the event of an attack with one of these agents. We have taken the botulism antitoxin program started by the Department of Defense in the early 1990s to completion and we are now building our antitoxin stockpile further. We have also built our stockpile of countermeasures to address the effects of radiation exposure with products such as Prussian Blue and diethylenetriaminepentaacetate, or DTPA. These countermeasures act to block uptake or remove radioactive elements such as cesium, thallium, or americium from the body after they are ingested or inhaled. Potassium iodide, a drug that can protect the thyroid from the harmful effects of radioactive iodine, is also in the Stockpile.

THE STRATEGIC APPROACH TO ADDRESSING MEDICAL COUNTERMEASURE GAPS

The initial focus of our efforts to protect the Nation was aimed largely at those threats that could do the greatest harm to the greatest number of our citizens, namely, smallpox and anthrax. A sense of urgency has pervaded our efforts and has defined new ways of doing business. Our new national security environment demanded accelerated product development timelines and new paradigms of interactions between industry and government with risk-sharing and enhanced intragovernmental collaboration. Using a robust interagency process, that mined intra- and extra-governmental expertise, requirements for medical countermeasures were identified, and options elaborated for addressing immediate and long-term needs. These experts continue to help us define the most expeditious way to traverse the critical pathway to develop and acquire usable countermeasures for the Strategic National Stockpile.

Application of the strategic approach: Anthrax

Although not transmissible from person-to-person, an attack involving the aerosol dissemination of anthrax spores, particularly in an urban setting, was considered by public health experts to have the potential for catastrophic effects similar to smallpox. . . . The potential for large-scale population exposure following aerosol release of anthrax spores, the threat demonstrated by the anthrax letters, and our knowledge that anthrax had been weaponized by state-actors, highlighted the nature of the treat. The Secretary of the Department of Homeland Security determined that anthrax posed a material threat to the Nation. And, because untreated inhalation anthrax is usually fatal, the Secretary of HHS identified anthrax as a significant threat to public health.

The approach to protect citizens against this threat demanded immediate, intermediate and long-term strategies and requirements. First, the existing stockpile of antibiotics in the Strategic National Stockpile was increased. Second, there was a need for a licensed vaccine to be used not only for pre-exposure protection for laboratory and other workers at known risk for anthrax, but for use along with antibiotics after an exposure to potentially decrease the currently recommended 60-day course of antibiotic therapy. Anthrax spores are stable in the environment and would have a profound impact if released in an urban population. Availability of a vaccine is a critical requirement for repopulation and restoration of the functionality of any exposed area.

The limitations inherent in the currently available anthrax vaccine were articulated in a 2002 Institute of Medicine report, "Anthrax Vaccine: Is It Safe? Does it

Work?" The report stated, ". . . a new vaccine, developed according to more modern principles of vaccinology, is urgently needed." An assessment of developing technologies was undertaken by HHS experts in the fall of 2001 and the decision was made that there was a sufficient scientific foundation, including a detailed understanding of the pathogenesis of anthrax and how anthrax vaccines provide protective immunity, to support the aggressive development of a next generation vaccine consisting of recombinant protective antigen (rPA). This research, spanning more than a decade from its inception in the early 1990s, was conducted in large part by the United States Army Medical Research Institute of Infectious Diseases at Fort Detrick, Maryland.

HHS defined a three-stage development and acquisition strategy with open competition for awards at each stage. The early and advanced development programs were supported by the National Institutes of Health's National Institute of Allergy and Infectious Diseases with contract awards in September 2002 and 2003, respectively. These were milestone-driven contracts with well-defined deliverables including the manufacture of clinical-grade vaccine and the conduct of Phase 1 and Phase 2 clinical trials. Large-scale manufacturing capacity would be required to support the civilian requirement for this medical countermeasure, which was defined through an interagency process to be the initial protection of up to 25 million persons. Senior officials throughout the United States government evaluated acquisition options to achieve this requirement and, in the fall of 2003, the decision was made to pursue the acquisition of rPA anthrax vaccine.

An evaluation of the status of the NIAID rPA anthrax vaccine development program suggested rPA vaccine could potentially become a licensed product within 8 years. In March 2004, the acquisition program for this vaccine, under the direction of my office, was launched using the Special Reserve Fund created in the fiscal year 2004 Department of Homeland Security appropriations bill. Utilizing a robust technical and business evaluation process, we reviewed multiple proposals and finally negotiated a contract with VaxGen of Brisbane, California, for 75 million doses of the vaccine, (anticipating a three-dose regimen). Using a milestone and deliverables approach utilized with the ACAM2000 smallpox vaccine development and acquisition program, and the rPA anthrax vaccine development related contracts at NIAID, the VaxGen contract lays out an ambitious program to include the delivery of the first 25 million usable vaccine doses to the Strategic National Stockpile within 2 years of contract award. A unique and critical aspect of the rPA vaccine BioShield acquisition contract is the fact that no payment is made until a usable product is delivered to the Stockpile. While awaiting delivery of this new vaccine to the Stockpile my office will complete negotiations for 5 million doses of the currently licensed anthrax vaccine in the next few days to support immediate requirements. Delivery of the product to the Stockpile will begin very soon after the contract award and will have a direct impact on our preparedness.

Other Needed Countermeasures

In an effort to fill other gaps in the Stockpile, we have made progress in contracting for products that will soon be delivered for use.

Potassium Iodide

In March 2005 a contract was awarded under Project BioShield for a pediatric liquid formulation of potassium iodide, a drug that helps limit risk of damage to the thyroid, from radioactive iodine. This formulation is aimed at young children who cannot take pills and are at the highest risk of harmful effects from exposure to radioactive iodine. This acquisition will provide needed protection for at least 1.7 million children. Product delivery will begin next month.

Ongoing Project BioShield activities

In addition to the Project BioShield acquisition contracts that have been awarded in the last 9 months, there are several other important BioShield procurement-related activities underway. We are reviewing the responses for Requests for Proposals for anthrax therapies, and we are continuing to move forward on the acquisition of an antitoxin treatment for botulism. Furthermore, to signal our intent to acquire a next generation smallpox vaccine, we will be releasing a draft request for proposal for industry comment within the next 2 weeks. Finally, in anticipation of yet to be determined requirements, we actively monitor the state of the medical countermeasure pipeline—both within and outside the government—by evaluating USG research and development portfolios and engaging industry through the publication of Requests for Information (RFIs). For example, we have recently released three RFIs to assess the timeline to maturity of medical countermeasures to treat nerve agent exposure, acute radiation syndrome, and additional products that might be available to treat anthrax. These requests are a key tool for HHS to dialogue

with industry partners and to inform the development of sound USG acquisition strategies.

Priority Setting Beyond Smallpox and Anthrax

The approach taken to rapidly expand our Nation's response capacity to meet the medical and public health impact of either a smallpox or anthrax attack demonstrate our national resolve to address these threats. But, in many ways, anthrax and smallpox represent the "low hanging fruit" for medical countermeasure research, development and acquisition and was enabled by a substantial research base developed by USAMRIID and NIH. There was consensus that these were our highest priorities and we had countermeasures available or relatively far along in the development pipeline to permit acquisition. Given an almost endless list of potential threats with finite resources to address them, prioritization is essential to focus our efforts. We rely heavily upon our interagency partner, the Department of Homeland Security, to provide us with a prioritized list of threats along with material threat assessments that will provide reasonable estimates of population exposure. This information is critical for future strategic decision making regarding how best to focus our National efforts in countermeasure development and acquisition, including whether in the short-term, the so-called "one-bug, one-drug" approach should continue while simultaneously investing in more broad-spectrum prevention and treatment approaches for the longer term.

Challenges to Rapidly Expanding the Strategic National Stockpile

Although defining priorities and quantifying the size of the threat to the population are the key steps to focus our efforts, we must be mindful of the realities of the spectrum of efforts needed along the research and development pipeline to produce a useable medical countermeasure. The process of defining required specifications for a countermeasure often reveals few, if any, candidates in the pipeline. Basic research and early development efforts, even when robustly funded, often take years before a concept is mature enough for advanced development. When a product has reached the advanced development stage, Project BioShield Act of 2004 provides an important incentive for manufacturers to take the product the rest of the way through the pipeline. And, as I have outlined here today, in the 9 months since Project BioShield was enacted, the incentive has sped final development of several products for the Stockpile.

Conclusion

In closing, I must emphasize that the number of threat agents against which we could guard ourselves is endless and new and emerging threats introduced by nature will present continuing challenges. Although we cannot be prepared for every threat, we have the ability to create a strategic approach to identifying and combating the greatest threats. HHS and its agencies including NIH, CDC, and FDA, have a clear mandate from President Bush and Congress to lead the charge in this arena. We have already made important strides and will continue to work to address the obstacles identified. Mr. Chairman, I look forward to working with you and members of the Subcommittee to address the challenges of bioterrorism preparedness and its impact on public health.

I will be happy to answer any questions you may have.

Senator GREGG. Thank you, gentlemen.

Let me start by saying I think there has been significant progress made. We started at zero, but I do not think we should underestimate how far we still have to go. We will start off by saying you have done a good job getting to where you are going, but the context of this hearing may ask questions about where do we have to go and how do we get there and why are we not there yet.

Let us begin. You, Mr. Simonson, talked about anthrax, and that is probably a good case study to look at because if you order the pathogens which are our biggest threat, smallpox is number one, followed by anthrax, and you have botulism. Then you actually drop down a level in my opinion and you hit botulism and hemorrhagic fever and a number of other things that are much more controllable than either anthrax or smallpox.

SYSTEM WEAKNESSES

But we have also seen three instances of what I would call real-life case studies as to how we react. We have got the SARS situation. We have got the avian flu situation, and we have just the simple flu vaccine situation. In each one of those instances, we saw weaknesses and we saw strengths of our system. I wanted to focus a little bit on the weaknesses because the strengths are good. Let me congratulate you for them, but I am concerned about the weaknesses.

The weaknesses, as I see it, are this. In the flu vaccination situation, we found ourselves with an "all the eggs in one basket" philosophy, and the provider of the vaccine turned out to be incapable of maintaining the supply. And thus, people were unable to get the vaccine. Are we creating the same problem again with anthrax, for example, where we essentially committed to a single supplier where the situation is that the supplier has not even gotten through clinical trials yet. Should we be approaching this by throwing the net wider and trying to energize more input to get more participation from more players?

We have one approved vaccine out there, which you mentioned you are buying 5 million doses from. It is a much more complex vaccine procedure than the one being proposed, but the one being proposed has not been approved, whereas the one that exists is approved. And so I guess my question is, why are we not splitting up at least into a couple baskets here rather than going full bore with one basket? That is the first question.

The second question is, are we energizing the minds out there that might have even more creative answers? Again, I will use anthrax as an example. I hate to be anecdotal because this should be more systematic than anecdotal. But I was up at Dartmouth where they have a very fine research facility, and the researchers up there said they were having great success with a proposal which basically addressed not only pre-prevention, but also if you were actually exposed to anthrax, had almost 100 percent recovery from anthrax. It was just at the mice level but they thought they were making great progress. But their attitude was they could not break into the system.

How many other people are out there? Are there people at Baylor? Are there people at Duke? Are there people out in Minnesota who basically have not figured out how to break into the system but might have the ideas? Are we energizing the research community first to come up with ideas and are we giving them a clear pathway that gets those ideas into the process, or are we shutting them out by simply choosing a winner here and saying this is the vaccine we are going to use, everybody else is off the table for the next 5 years because all the money is committed to this vaccine?

So it is two levels of questions. Have we made technically the right decision by choosing one vaccine to basically put all our eggs in one basket in light of the flu experience? And secondly, in doing that, have we also shut down the creativity in this area of anthrax because everybody now says, well, the anthrax is off the table because they have chosen this vaccine? So people at Dartmouth, peo-

ple at Baylor, people at Duke are going to move on to something else.

Mr. SIMONSON. I think, Senator, the influenza situation and other situations where we have put all of our eggs in one basket is distinguishable from what we are doing on anthrax. Utilizing what we sometimes call the push-pull, you push scientific development along the way using NIH and other instrumentalities to the point where it is far enough along that a Government contract can incentivize a maker to pull it. That is a very delicate balance in the negotiations with these companies. We found in our negotiations with the contractor that got the award that the $75 million was about what we needed to pull it and——

Senator GREGG. How much does that constitute in dollar value?

Mr. SIMONSON. $877 million.

That was the pull needed to get there. Cutting it in half would have really limited our ability to take advantage of the economies of scale and so forth as you ramp up.

But I think our interest in acquiring more AVA BioPort vaccine shows we are seeking not to put all of our eggs in one basket. Hopefully, we will be finishing the 5 million dose contract very soon. There is an option in there for another 5 million doses. It keeps the door open and allows us to continue a dialogue with BioPort so we can, where appropriate, adjust our stockpiles there.

Plus, we are doing some other things that are related. We have enormous quantities of antibiotics effective against anthrax.

We are trying to develop a good anthrax therapeutic, and this procurement I think especially speaks to the situation you mentioned earlier about people feeling locked out. What we have said is in order to keep our acquisition in sort of the state of the art, we are going to engage in essentially a three-stage acquisition, acquire the first round of anthrax therapeutics, but keep RFPs open for the next 2 years so products that were not able to compete in the first round could compete in the second round so that we have a diverse portfolio of anthrax therapeutics. So it was specifically designed for the purpose of not locking out someone who was on the verge of a breakthrough but had not quite gotten to the point where he could meaningfully compete for a BioShield contract. So we are sensitive to that.

I am not sure we are doing it the right way. I am not saying we are fully satisfied with the experience, but I think we are learning as we go and we are trying to be good stewards and to not overcommit where we do not see a need to. But we are sensitive to the need to keep the scientific community energized and interested in breakthroughs.

Senator GREGG. Senator Byrd.

CHEMICAL AND BIOLOGICAL AGENTS

Senator BYRD. The Gilmore Commission in its December 15, 2003, report stated that a single biological or nuclear attack could realistically kill tens of thousands of people. The report went on to say that to meet today's threats, we need technological breakthroughs such as the development of sensors to detect deadly chemicals or biological agents.

I believe that is your area, Dr. Albright. What are you doing to prevent these deadly agents from crossing our borders, coming into our ports, or arriving by plane?

When Secretary Ridge testified before the subcommittee last year, he said if a passenger wanted to board a plane with a biological or chemical weapon, we do not have the capacity to detect it. Is that still the situation? Does your budget request address this issue?

Dr. ALBRIGHT. So there were a couple questions. To answer the second question, the answer is no, we do not have a good way of detecting someone trying to bring a vial of pathogen across the border. That would be an extraordinarily difficult technical problem to address. If you think about the amount, for example, of anthrax or of smallpox needed to be brought across the border in order to either affect a large number of people or to act as seed stock for a domestic capability, you do not really need very much. The amount of the actual anthrax you would need would be about the size of a quarter. You would need very little smallpox to start culturing seed stock.

So the approach we have taken is rather than trying to solve what appears to be an intractable problem at the borders, let me stop and say there is another side to this, and that is when people and cargo do cross our borders, to the extent that we are able to target suspicious individuals or suspicious cargo and then inspect them manually and thoroughly, that would certainly provide a venue, just as it would provide a venue for detecting almost anything else they would bring across the border. But looking for, as I said, a vial of anthrax, the technical obstacles to that are just extraordinary.

So the approach we have taken instead is rather to detect an attack when it occurs because, in a sense, one of the real dangers or terrors associated with these kinds of pathogens is if they are deployed covertly, they start to infect people before anybody really knows what has happened. And by the time you start to see symptoms, it is usually too late to do much about it. So the trick here is to detect the attack before people become symptomatic, and when we have an opportunity, deploy the stockpile and treat the individuals concerned and save them.

BUDGET REQUEST

Senator BYRD. Would you touch upon the other question I asked? Does your budget request address this issue?

Dr. ALBRIGHT. Yes, sir. Our budget request I believe is approximately $80-odd million for the next generation of the BioWatch. These are the urban detection systems. We have also got about $100 million in our budget, roughly that is operations in support for the current system and actually there is another generation being deployed as we speak.

CHEMICAL DETECTORS

Senator BYRD. The Department is spending over $100 million on the system of sensors known as BioWatch. The budget request for fiscal year 2006 proposes over $225 million for a new office called the Domestic Nuclear Detection Office.

Less clear are the Department's efforts to prevent a chemical attack. After 9/11, the Senate approved $15 million for the D.C. Metro system to deploy chemical detectors in the D.C. subway system. Now, that is an excellent system. It gives Metro the capacity to immediately determine if the subway has been exposed to a chemical agent so it can effectively respond.

This funding was included at Congress' initiative. It was not requested by the President. In fact, the White House specifically objected to the funding, describing it as excessive.

Last year, Under Secretary McQueary listed the D.C. Metro project as an accomplishment.

Is there any funding in the President's budget to take advantage of the lessons learned from this pilot program to deploy the chemical detectors in other large subway systems or urban areas around the country?

Dr. ALBRIGHT. The short answer is yes. Let me explain to you how it works.

First, it is called the PROTECT System, the system we have in the Washington Metro system. We see it as a significant success. In fact, the Department of Homeland Security is no longer really involved with it. We turned it over to the Washington Metropolitan Area Transit Authority. They operate it to the extent they need technical assistance, which is almost never, we supply it for them, but this is something that has been completely transitioned.

I will also add that during both the Republican and Democratic national conventions, we deployed this system also to the subway systems in Boston and in New York, and in fact, at the specific request of the New York Transit Authority police, we have kept the system deployed at certain sites in the New York subway system.

The way it works, though, is that from our perspective, the technology development is finished. So now the question here is one of transition. How does one do that? In particular, how does one transition these technologies to transit authorities which are local government entities?

So what we have been doing is working very closely with the Office of Domestic Preparedness, with ODP, to create grant guidance that will allow and focus grants to be deployed in local metro systems. There are something like over 30 metro systems around the country. They would then basically take the system and install it. It is really very inexpensive. It is only a few million dollars per metro system that is needed to do this. So that work is underway, but that would be embedded within our overall grant budget.

Senator BYRD. My time is up. Thank you, Mr. Secretary.

Senator GREGG. Thank you. Again, I recognize the chairman of the full committee.

NEW PRODUCTS TO PROTECT AGAINST BIOTERRORISM ACTS

Senator COCHRAN. Mr. Chairman, I just have a couple of questions. One is to focus attention on how we are developing incentives for researchers to discover and develop new products to protect the general public against bioterrorism acts. Dr. Albright, what are we doing and what is in the budget to try to help reach that goal?

Dr. ALBRIGHT. In terms of fundamental research for medical countermeasures, sits within the realm of my colleague here, Mr.

Simonson, and the Department of Health and Human Services. I will point out they have well over $1 billion devoted to research and development activities within NIAID to invoke intramural and extramural contracts, and by that, I mean to researchers within NIAID, as well as to universities to develop the scientific basis for countering these threats across the entire list of category A and even B and C agents.

Senator COCHRAN. Mr. Simonson, do you have a response?

Mr. SIMONSON. That is absolutely right. We have about $1.7 billion assigned to the biodefense research portfolio at NIH. It is a very aggressive agenda there to move advancement forward.

Senator COCHRAN. Will this utilize expertise that we have at academic health science centers, specifically the drug discovery efforts of schools of pharmacy?

Mr. SIMONSON. The extramural program does leverage academic health centers. I will check this for certain, but I would be shocked if discoveries in schools of pharmacology did not leverage some of this money.

SYSTEMS THAT MONITOR SUPPLY OF PHARMACEUTICAL PRODUCTS

Senator COCHRAN. I know there are efforts underway at the Centers for Disease Control and other agencies to develop systems that monitor the supply of pharmaceutical products besides those already in the strategic stockpile that could be needed in the event of widespread bioterrorism attack. Mr. Simonson, can you comment on such systems?

Mr. SIMONSON. Yes. CDC, through the Strategic National Stockpile, has a monitoring function where we are looking for availability in the both reverse distribution and distribution system, in case something happens where we would have to leverage what is already out in the field.

The FDA has a drug shortage function where they are tracking vulnerabilities in the pharmaceutical industry, how much of a particular product is out there and could be used in an emergency.

The difference is FDA has access to very closely held proprietary data that CDC often does not have access to. So we work it together.

Senator COCHRAN. Is there a sufficient amount of money in the budget request to get us started, Dr. Albright, to develop the infrastructure, the facilities for continued research in an aggressive way to meet this challenge?

Dr. ALBRIGHT. I think certainly in our fiscal year 2006 budget request, the answer is yes. There are multiple aspects to your question. Certainly in the research side, again that would be in DHHS, but there have been funds actually appropriated in 2004, for example, for the development of the laboratory infrastructure, the capitalization, for example, of biosafety level 4 research facilities across the country, and it is my understanding is well underway.

There are other issues, though. One of the things that Mr. Simonson and I have been working closely with is some of the capitalization needs associated with the developmental process. There are some unique issues associated with putting some of these bioterror pathogens through clinical trials, or the equivalent of clinical trials, because obviously we do not infect human beings with these

diseases in order to test them, that we are actively discussing at the moment.

Senator COCHRAN. Thank you, Mr. Chairman.

Senator GREGG. Thank you.

Senator Craig.

SHELF SENSITIVE VACCINES

Senator CRAIG. Mr. Chairman, thank you very much.

You touched upon a subject I want to pursue with our panel, and gentlemen, you are the professionals here. You tell me if this is an area that does not pertain to this particular area.

In the last several years, I chaired the Select Committee on Aging and a week before Chiron announced its Liverpool plant had been shut down, they were before us telling us they were going to meet the necessary 100 million doses, or whatever the number was, for the flu season. They did not meet it. We got through that season.

But it exposed to us the vulnerability of that particular vaccine industry, and it was a product, in part, because of what had transpired over a course of years. Here you have a mutating virus, I believe, and it changes annually, and you cannot stockpile, and so you have to predict and produce. If you mispredict, you end up with a lot more doses and it bankrupts your company and you go away. And you find out it is much too expensive to play in that field of health care, if you will, unless it is incentivized by government.

Of course, that technology is an egg-driven culture technology, and we are not into cell technology yet. We are trying to get money there.

The bottom line is we made it through this last season. I do not know that a flu virus could be brought to this country effectively and spread to create a pandemic by a terrorist organization. You are the ones who would have to be able to tell us that, whether it was a doable proposition.

But if it were, we would be so unprepared at this time to deal with it by all situations, and in certain segments of our country, certain demographics, the elderly, flu can be lethal, as we know, losing thousands and thousands of them in a normal flu season.

We are trying to correct that problem, but we are not quite there yet. Government is simply going to have to help these companies and buy off the surplus at the end of the season to allow them to produce.

Senator COCHRAN. How many of these kinds of vaccines or treatments are we preparing that are shelf-sensitive, that have to be rotated on an annual basis, that have to be sensitized to the mutating viruses all the time to be good and usable?

Mr. SIMONSON. Flu is the only vaccine that has to be made in this campaign process.

Senator CRAIG. Is it transportable and can it be used as a weapon?

Mr. SIMONSON. Influenza?

Senator CRAIG. Yes.

Mr. SIMONSON. One would think so, yes.

Senator CRAIG. Would you agree we are totally unprepared if it were ever used in that situation?

Mr. SIMONSON. I am not sure I would say we are totally unprepared, but it presents an enormous challenge to us and it is something we have been mindful of and worried about I think since the President took office.

Senator CRAIG. We are proceeding into the next flu season with how many producers of flu vaccine? Two?

Mr. SIMONSON. There are two producers of the killed vaccine, one producer of the live attenuated vaccine, and a third on the horizon. There is still regulatory work occurring with respect to the third.

CELL TECHNOLOGY VERSUS CULTURE TECHNOLOGY

Senator CRAIG. How much investment are we making in the new cell technology versus, if you will, the culture technology of eggs?

Mr. SIMONSON. We entered into a $97 million contract for tissue culture, cell culture technology, which has enormous benefits over the embryonated hen's egg approach.

Senator CRAIG. And that benefit is to be able to speed up a process ultimately to produce a vaccine more quickly. Is that not correct?

Mr. SIMONSON. More quickly and it is less vulnerable to the things chickens are vulnerable to. We have hundreds of thousands of chickens who lay eggs for our vaccine every year. A high path influenza virus, avian influenza virus——

Senator CRAIG. Clean chickens.

Mr. SIMONSON. Yes, but they are still susceptible to disease. So it has worked out so far, but it is a fragile infrastructure.

We have also developed over the last 6 months some contingencies for our chicken flocks. We are building up flocks so if we have a problem in one, we can supplement with another, and we can also produce year around.

Senator CRAIG. But you have a tremendous time spread in that technology compared to tissue. Is that not correct?

Mr. SIMONSON. That is right.

Senator CRAIG. Well, I hope you are putting money into that new technology. We lucked out this year. We made it through the season with a lot of cooperation and, frankly, a lot of good coordination on the part of NIH and others and a lot of communities of interest. But I was absolutely amazed at our vulnerability in that area and the unwillingness, at least of Congress to date, to recognize it and incentivize it so we can keep industries functioning in those areas, not just in influenza but in other childhood areas. There is the liability issue, along with a lot of other things, that have just simply caused them to leave the market.

Mr. SIMONSON. Even before 9/11, this was a very clear priority of the Bush administration. There was work going forward even before 9/11 on this. There is so much more to be done, but we have made a very good start I think. But it was, for decades, neglected as a seasonal nuisance, the flu, and the flu is not a seasonal nuisance. The flu is, in some ways, a very, very unique threat to us if you look back at 1918 and what that did to this country, and we have to prepare for that and we are.

Senator CRAIG. Thank you.

Senator GREGG. Senator Stevens.

ADVANCE APPROPRIATION

Senator STEVENS. Thank you very much, Mr. Chairman.

I was pleased to join you in introducing this basic bill on BioShield, Senator Gregg. We gave an advance appropriation of $5,593,000,000. How much of that has been allocated to you for 2005? That was for the years 2004 to 2013. I just wondered how much has been released to you.

Mr. SIMONSON. Well, $2.5 billion has been released to us.

DEMONSTRATION OF IDEAS BY PEOPLE

Senator STEVENS. We had a sense of urgency in terms of your mission. Part of it came from the fact that I was chairman of appropriations. Senator Cochran is now, and he is going to have this delightful experience. But people came to me to demonstrate some of the things they said they had prepared. One gentleman told me he had a substance which, if it was injected into the leg of an individual, would guarantee protection against all substances for a period of 48 hours. Now, I sent them to see you. What do you do with people like that when they come in?

Mr. SIMONSON. Well, there are a number of these people.

Senator STEVENS. There are a great number of people, but somewhere there might be one who knows what he is doing. That is what I want to know. What do you do with them?

Mr. SIMONSON. I hold out that hope as well. So what we do is we gather the research and development types, the physicians and scientists, in my office who have the capability of seeing maybe a gem in the rough and we go through it. In fact, we do this, I would say, in the regular course of business. We are going to be doing it again next week with a provider, a stem to stern review of what they say will protect against, in this case, irradiation exposure.

But it does happen often. We do it, and if we think there is any hope for it, we bring in our colleagues from NIH. We are looking all the time for more. Sometimes they are stacked up a little bit, but we do get to the people who come forward with these ideas.

Senator STEVENS. Is Dr. Franz still out there?

Senator GREGG. He has not testified yet.

Senator STEVENS. He has not testified yet. Can I ask him a question?

Senator GREGG. You can, sure.

NONGOVERNMENTAL SCREENING GROUP

Senator STEVENS. Do you think there should be a nongovernmental screening group that people will know exists that could review suggestions like this coming from individual scientists?

Dr. FRANZ. I'm sorry, sir. A nongovernmental screening group?

Senator STEVENS. Yes. Should we have provided for such an entity in the bill that we passed, a nongovernmental screening entity to review these suggestions so it would be quickly reviewed?

Dr. FRANZ. I think it depends on the resources. My own experience was as the Commander of the USAMRIID, we used to receive a lot of these things, and for the most part, as Mr. Simonson has said, I believe it is possible to look at the data presented, and oftentimes it is scanty. And to sit down with some smart people with

both basic research and clinical experience and make a decision to do a very careful screening, using good laboratory practices and so on, of each of these products would be very, very expensive. So I think it is important there be some kind of careful look outside the laboratory by some smart people before we send them to the laboratory.

Senator STEVENS. Thank you.

Mr. Simonson, my only comment is it just sounds to me there are a great many people in our national community who are thinking about these threats and some of them have capability and others do not. But I do hope we find some way to have an identification of where these people can take their suggestions. I am sure Senator Cochran will appreciate this because they still keep coming to us for money and we do not know one single thing about what they are talking about. So I do think there ought to be some identifiable place where people with capability and ingenuity to try to help solve some of these problems could go and know who they are talking to and we could know who to send them to.

Mr. SIMONSON. There is one other mechanism we use, as I indicated earlier. This request for information. We will take a look at what is missing and having looked through the Government pipeline, seeing nothing, we will send out a request for information, sources sought. Do you have work in this area that might be useful to the Government? And that produces a fair amount of really reliable data that we can then move forward on. So we are trying to do that.

I think there is no question, Senator, that when it comes to security countermeasures, people coming forward and saying we have got these ideas and we need a place to go, ours is the place to go. We want to have an open door for those sorts of inquiries.

Senator STEVENS. Thank you very much. My only comment would be if I let someone study how many permits the Wright brothers would have had to proceed with the demonstrations down at Kill Devil Hills, it would amaze you how many they would have had. I am sure similar things apply in this area. There is just an overwhelming number of permits necessary for anyone to even proceed with this independently. So I do hope we find some way to accommodate the knowledge of some people who may have the ingenuity to think a lot better than we thought they could.

Senator GREGG. Senator Allard.

Senator ALLARD. Thank you, Mr. Chairman.

BIOTERRORISM AND COOPERATIVE EFFORTS

I would like to make an inquiry as to how your efforts against bioterrorism are being coordinated with the Department of Defense, as well as the CDC lab? They are all deeply involved in biological threats to this country either through an epidemic, what we naturally have occurring in this country, which may be introduced or could be used by other nations as far as a bioweapon is concerned. I wonder if you might comment about your cooperative efforts, if you would, please.

Mr. SIMONSON. We have a structure in place that Dr. Albright and I, Dr. Winkenwerder, Assistant Secretary for Health Affairs at the Department of Defense, and Dr. Kline, who is Assistant to Sec-

retary Rumsfeld for chemical and radiological and nuclear matters. The four of us chair an interagency group that works through these countermeasure issues, set requirements, and make sure the right hand knows what the left is doing because there is a fair amount going on outside of HHS laboratories. Parny may have something to add to this, but I think that really is where all the coordination is occurring right now on the countermeasure development front.

Senator ALLARD. Are you communicating with the Department of Agriculture's plant and animal infectious diseases also? That is anthrax and potentially plague and zoonotic diseases. I assume you are also communicating with them.

Mr. SIMONSON. Yes. They participate in this group.

INTRODUCTION OF DISEASES FROM OTHER COUNTRIES

Senator ALLARD. Now, I understand the chairman had some questions he raised about flu. I was not sure whether he was talking about just the regular variety of flu that affects humans or he was talking about the avian influenza, which does not occur in this country but causing some deaths in Asia and apparently is pretty virulent and is a disease that is of serious concern to get introduced in this country.

When you have those kind of reports, what kind of action do you take?

Mr. SIMONSON. The first thing we do is to ensure that we are getting reliable data out of the region.

Senator ALLARD. So we send scientists down there to confirm the diagnosis.

Mr. SIMONSON. We do send people there. We also bring material back to the CDC or other laboratories to make sure the sample is being properly evaluated and that we are watching for antigenic drift, changes in the characteristics of the disease.

We fund, directly through the World Health Organization (WHO) or through bilateral agreements, ways to improve surveillance in these countries that have minimal infrastructure.

The United Kingdom and the United States fund a transport fund to actually pay for isolates to be shipped out of these countries that cannot afford to ship them, believe it or not. It is a very expensive proposition.

So that is the first thing we do. We trim that up. We send doctors into the field working with the WHO.

I think the second thing we do, this is something Secretary Levitt has been very committed to doing, is work diplomatically with his counterparts, health ministers and so forth to underscore the importance of transparency because without transparency, none of this is going to do us any good. We are trying to back up that transparency with funding.

Senator ALLARD. Well, the importation of material that is infected or potentially infected is a very volatile issue. We have a research laboratory off the shores of this country so we can make a claim that the disease does not occur in this country. I would hope that when you are bringing in those types of materials some consultation be made that in this particular case we happen to be talking about animal diseases, and it is important on our trade agreements that we never and we can always make the claim the dis-

ease does not occur in the United States. And avian influenza can have a dramatic impact, for example, in the poultry industry if we cannot make that claim as far as import and international trade and everything.

So I would encourage you, if you are not, to work closely with those various agencies because we are trying to do what is necessary to protect our population. We need to study. We need to be prepared for them, but yet we have to be careful in what way we set up our studies and how we handle that kind of material. It can be very complicated and it could be very controversial.

Mr. SIMONSON. I just want to follow up on something I said a moment ago. When we bring material back into this country, it is done in a very high level of bio-security so that we do not have to worry about it getting out, much like when other agents are brought back——

Senator ALLARD. Very, very important. Thank you.

Thank you, Mr. Chairman.

Senator GREGG. Thank you. I want to thank the panel.

I think Senator Stevens' point that we need to formalize the point of access where people of ideas can go is a pretty valid one because I know I hear it too. I have people come to me and say I have got a solution to this problem, and I refer them. It would be nice, I think, if we could pick a central Government place where we could send all these people who have those good ideas. I guess yours is the shop. I am not sure how we make it more visible in that area, but I think that might be useful.

But we do appreciate your work and we thank you for your time this morning and appreciate your testifying.

We are going to now move on to the second panel which is folks who are outside the Government right now and who have expertise as to whether or not we are doing a good job as a Government and who have a lot of experience, beginning of course with Dr. Franz, who has already been drawn into the discussion here, which we very much appreciate. Hopefully we can get the electronics here to work well so we do not end up with a lot of interference. Dr. Franz we know well because he was head of the U.S. Army Medical Research and Materiel Command for 23 years. He is now active in a number of other activities.

We have Dr. Leighton Read, who has joined the Alloy Ventures as a general partner in October 2001. He has 14 years as a biotechnical entrepreneur and investor, and he is going to give us his thoughts as to how you get into this business and whether or not the Government is making it easy.

And we have Mr. John Clerici who is an expert in liability issues. He was Judge Advocate in the United States Air Force where he spent a considerable amount of time advising the Air Force research laboratories on how to procure technologies.

So we appreciate all of you taking the time to be with us today. What we are interested in hearing about is how you think the Government is doing in instituting the goals of BioShield, which have certainly been outlined rather thoroughly this morning, to prepare ourselves to deal with a biological/chemical attack and to anticipate what the problems would be and be ready to deal with them. So we want to hear your thoughts on this.

We will start with you. Why do we not start with Dr. Franz and make sure we have got this thing working so that he is up and running. Dr. Franz is in Boston, which is obvious because there is a Red Sox symbol in front of him, probably curing Red Sox fever. If you could give us a test, Dr. Franz, that would be good.

Dr. FRANZ. Good morning, sir. Can you hear me?

Senator GREGG. Yes, we can. Thank you. Why do you not proceed?

STATEMENT OF DR. DAVID FRANZ, CHIEF BIOLOGICAL SCIENTIST, THE MIDWEST RESEARCH INSTITUTE

Dr. FRANZ. Mr. Chairman, distinguished members, it is an honor to appear before you to address issues related to the procurement of medical countermeasures to protect the American population from bioterrorist agents and emerging infectious disease. I am currently Senior Biological Scientist at the Midwest Research Institute in Kansas City. I believe you have my resume.

This committee has asked that I provide some broad perspective on the medical aspects of biological defense in the context of a world in which intentional release of biological agents is of significant concern and natural introduction of disease is a reality. I will make seven brief points that encapsulate my written statement and then summarize my thoughts regarding the implications of these points for the challenges at hand.

First, regarding the threat, I believe the most significant barriers to biological terrorism today is the intention to commit the crime. This is especially true for contagious viruses. In the future, technology will draw on the options for both protection and for abuse.

Second, we are extremely vulnerable to bioterrorist attack in this free society, but for many technical and behavioral reasons measuring actual risk to any segment of the American population or its agriculture will continue to be extremely difficult.

Third, biology is characterized by great diversity. Microbes like our own immune systems can be either strong or weak. We can rank microbial capabilities that cause disease and even their utility for terrorist exploitations, but without solid intelligence, we can never know for sure which specific biological agent we might face or when. Many of us agree, however, as was mentioned earlier, there are outliers among the diverse microbial population. These include organisms that cause smallpox, anthrax, and foot and mouth disease.

Fourth, biology is neither as crisp nor are the rules of play as well defined as they are for physics and chemistry. Therefore, there are many opinions regarding the way ahead for bioterrorism defense.

Fifth, just trying to decide how to organize to protect ourselves is challenging. Secretary Richard Danzig has proposed a handful of select scenarios to be used "as an anvil against which to hammer our ideas." A compatible approach, which I have often discussed, is to prepare for the outliers and then broadly enhance our public health system as if we were expecting an unknown emerging infectious disease.

Sixth, regarding future threats, we should assume that almost anything is or will be possible, but we must not forget just because

it is theoretically possible it is almost always harder for us to manipulate biology either for good or for ill than we predicted.

And finally, seventh, we can do many things to protect ourselves but our preparation can never be perfect. I believe it is critically important that we carefully craft our concept of use and application of various biodefense measures are being developed so we address the greatest risks and vulnerabilities and ensure the maximum benefit for our investments. It will be costly, but the cost of failure in this area is potentially enormous. So how can we apply these principles?

First for vaccines. It is relatively easy to justify the acquisition of vaccines for anthrax and smallpox for the population. It is important, however, we thoroughly understand our concepts of use as we attempt to develop traditional agent-specific vaccines for the civilian population. In the short term, we should exploit next generation, flexible vaccine platforms. We were working on these in USAMRIID in the mid-1990's already, which will allow us relatively quickly to produce a licensed product, counter an outbreak of either epidemic or even pandemic. The basic platform might be licensed for use in humans now, allowing us to simply add a genetic cassette when a new vaccine is needed, greatly shortening the time for use. Our current system of vaccine research, development, and approval is simply not flexible enough to respond to terrorist attack or emerging disease.

For drugs, it is difficult to argue against spending as much as we can afford on antivirals and new classes of antibiotics and exploiting the genomic revolution to develop new categories of anti-infectives. All of these will improve the lives of Americans with or without a bioterrorist attack.

And regarding the future, attempting to protect our population from the unknown threat of today and especially of tomorrow with specific countermeasures like traditional vaccines will likely be extremely costly and inefficient. Significantly boosting the immune system to give us broad, multi-agent protection is now slightly more than a great idea I believe. I will not be surprised if it will be 15 or 20 years before we can do this in domestic animals effectively and maybe 30 years before we can really make a difference in the broad population of humans. But I believe we must be doing the necessary research right now. We probably do not yet know how much difference attempts to turn up the gain on our own immune systems will make. It is likely that for prophylactic use in a broad population where side effects may be totally unacceptable, the value could be minimal. However, in select populations or the already exposed or ill, where non-life-threatening side effects are accepted, this class of countermeasures may be significantly more effective. We actually have examples of use in individual patients with cancer and hepatitis today, but our tools are still very, very crude.

Finally, regarding market drivers for medical countermeasures, my experience is second-hand and limited. I believe specific countermeasures for most bioterrorism agents and probably for briefly emerging infectious diseases will, for the most part, require Government funding. For those countermeasures that have broader application, a significant portion of the research will still probably be

funded by the Government. However, advanced development and even production will be of interest to industry, I am sure. Even there, incentives may be helpful or necessary in driving development and production of certain compounds.

PREPARED STATEMENT

Again, I appreciate the opportunity to present this information before the committee. I worked hard to keep our leading national laboratory for the development of medical countermeasures for the force solvent through the 1990's. I know it is not easy to convince someone that medical countermeasures for a poorly understood threat of unknown risk are really important. The field of the vaccine and antiviral drugs requires both science and imagination, a phenomenal personal dedication by scientists and shepherding over enormous regulatory hurdles. And when it is completed, you cannot paint on the national colors and sail it around the world or even fly it over the Super Bowl at half-time. When it is finally licensed, the administration of that vaccine is often dreaded by the healthy recipient whose very life you want to save.

Thank you for your important work and for this opportunity. I'd be happy to answer any questions.

[The statement follows:]

PREPARED STATEMENT OF DR. DAVID FRANZ

Medical Countermeasures to Biological Threats—and Emerging Infectious Disease

Mr. Chairman, distinguished Members, it is an honor to appear before you to address issues related to the research, development and procurement of medical countermeasures to protect the American population from bioterrorist agents and emerging disease. I am currently the Senior Biological Scientist at the Midwest Research Institute in Kansas City. I served on active duty in the U.S. Army from 1971 to 1998, with 24 of those years in the U.S. Army Medical Research and Materiel Command. I served for 11 years at the U.S. Army Medical Research Institute of Infectious Disease, which I commanded before my retirement. I currently serve on a number of senior S&T advisory panels for the Department of Defense and Department of Homeland Security.

This committee has asked that I provide some broad perspective on the medical aspects of biological defense in the context of a world in which intentional release of biological threat agents is of significant concern and natural introduction of disease is a reality. I have attempted to provide my views on a number of these issues below.

What is the nature of the bioterrorist threat?

Biological terrorism is a unique threat to our society, our economy and our freedom. Like the biological warfare threat of a decade ago, dual-use facilities and technologies may be exploited to make terrorist weapons. Although we have improved our defensive capability, we can still not yet, geographically or temporally, warn our citizens of an attack in time to take evasive or protective action. Unlike biological warfare, the production facility' and the weapon of the bioterrorist may be very small indeed. Finally, as we have learned since October 2001, attribution of a small scale attack can be very difficult or impossible. Furthermore, the microbes are generally widespread in nature and the technological tools are rapidly improving in capability and availability worldwide. Neither the microbes nor the tools to manipulate them can be outlawed, the former because if their ubiquity and the latter because of their value to society. Therefore, it is possible to easily hide a biological terrorist program. With proper agent selection there could be minimal technical hurdles. The most significant barrier to the biological terrorist today—and for the foreseeable future—is the intention to commit the crime.

Can we measure the risk?

We know that our human and livestock populations are extremely vulnerable; this is a function of our free society and our well-developed livestock industry. We know

that the impact of an intentional attack with microbes could be enormous, measured in human lives or dollars lost. We know there are groups and individuals who threaten us and we have some sense of their abilities with things biological. Our understanding of the all-important factors of intent and motivation is much less clear. Therefore, risk—where all these variables come together—is only poorly understood. The president's directive "Biodefense for the 21st Century" specifically calls for a biological risk assessment to be performed every two years, so that our national response to the threats, vulnerabilities and consequences of bioterrorism can be improved. This risk assessment presents technical challenges that are being addressed by the Department of Homeland Security.

Are some agents to be feared more than others?

Biology is characterized by great diversity. Microbes of a given genus or family may be strong or weak. Species, subspecies or strains within a genus or family may be stronger or weaker than their near relatives. We call variola virus (the agent of smallpox), Bacillus anthracis bacterium, the foot and mouth disease virus and maybe even the toxin, botulinum, "outliers" because they can cause severe disease in humans or impact animal populations. Even that is an oversimplification. Botulinum isn't botulinum and anthrax isn't anthrax. All of these organisms, or the toxins they produce, live on a spectrum with regard to the pathology they can cause in humans or animals: some weaker; some stronger. To be an agent of concern' the bug need not only be able to cause disease in humans or animals, but must also have the right combination of a series of important characteristics, for example: stability, transmissibility, easy producability and/or the ability to overcome countermeasures. With regard to catastrophic bioterrorism, we may be truly concerned about less than 1 percent of those microbes found in nature. Yet, that's enough! The lesson for us is that we can—at least to some degree—prioritize the agents for which we use our resources to develop countermeasures. However, without solid intelligence, we can never know for sure which one we will face.

What is the impact of all this variability in biology?

If we were able to plot all known microbes in the world on a graph with their name stacked up on the vertical (Y) axis and their relative ability to hurt us spread across on the horizontal (X) axis, we would get some kind of a curve. Let's assume the curve would be roughly bell-shaped with a small number of microbes having very low ability to cause disease, most of them with moderate ability to cause disease and few which can cause severe disease. We could do the same thing with stability, transmissibility and the ease with which they can be produced. If that isn't enough, we could plot all Americans on a similar curve, describing the relative ability of their natural immune systems to combat disease of various kinds. Some of us are strong and some are weak, but most of us are average in ability to withstand exposure to disease. More than half of us might survive exposure to smallpox, without any medical help, but maybe only a few percent of us would survive inhalational anthrax. To complicate the picture even further, the outcome of some exposures is dose-dependant. This is especially true of the toxins, which don't replicate within out bodies, but act more like chemicals. Biology is just not as crisp and clean as physics or even chemistry; this is one reason we have heard so many opinions about protecting our citizens from biological terrorism.

How can we decide what to protect ourselves against?

The short answer is, "We can't". However, certain bugs are much better suited as weapons than others: B. anthracis, because of it's ability to survive in a spore form for many years; variola virus, because of its ability to spread from person to person and foot and mouth disease virus because of the way it can sweep through an agricultural economy so quickly that its point of introduction may be difficult to discern. We have recognized those and either have dealt with the outliers or are in the process of dealing with them specifically—as we should.

Richard Danzig has proposed another scheme in his excellent document entitled, "Catastrophic Bioterrorism: What is to be done?" His approach involves a short set of specific agent release or introduction scenarios, which if prepared for properly will likely give us many of the tools and capabilities to deal with most other agents which have characteristics similar to those we specifically prepared for. Several of our government departments and agencies responsible have implemented Secretary Danzig's approach.

Another model which I, and others, have put forward—after taking anthrax and smallpox off the table with specific countermeasures—is to think about the unknown as emerging infectious disease and take general steps such as establishing surveillance systems, upgrading diagnostics capabilities and educating healthcare providers regarding outbreak response. Eliminating vulnerabilities in our public

health system is not difficult to justify, and has a beneficial "dual use". I have characterized this way of thinking about preparation by the simple equation, Bioterrorism—Emerging Infectious Disease + Intent. We don't know when we will face a bioterrorist attack, but history tells us that we should expect emergence and re-emergence of "exotic" diseases every few years in the United States. If we prepare our public health system to deal with these types of occurrences, we will be far better prepared to deal with a bioterrorist attack.

What about future threats?

We believe that multiple-drug-resistant bacteria were produced by the Soviets before the genomic era. We know that foreign genes can be added to both bacteria and viruses, making avirulent agents virulent, or conferring additional properties of virulence or pathogenicity. We know that the tropism—the virion's preference regarding the body's cells it infects—can be changed. We know that nature can change an animal pathogen so that it infects humans. In the biology of microbes, we should assume that almost anything is possible. That does not mean that it will be done by a human—but we are entering an era in which all these manipulations and more will become easier.

Can we place a value on classes of countermeasures?

We can do many things to protect ourselves from a bioterrorist and his bugs; they range from political and behavioral actions to change intention in those who might harm us, or to undermine their support where they live, to medical solutions like vaccines and drugs, physical devices such as protective masks that filter microbes out of the air we breath, or monitoring systems to detect an attack on high population densities. All have a place in our integrated national defense, but not all are equally suitable for all populations we must protect—or deter—OR for every agent we wish to protect against. The Nunn-Lugar Cooperative Threat Reduction program has had a very significant positive result among the now-aging weaponeers of the FSU, but we would not expect the same model to work with Al Quiada. A protective mask will be of much greater utility to a soldier on the battlefield than a businessman in Boston, because we don't have, and probably can't afford, the capability to tell the business man when to don it. A vaccine against plague will more likely be useful to a Marine than a housewife, for behavioral and cost reasons. A currently-available antibiotic may be of great utility after an anthrax attack and useless after the release of highly-pathogenic avian flu virus that has been adapted to infect humans. We need to carefully craft our concept of use and application of the various biodefense measures that are being developed so that we address the greatest risks and ensure the maximum benefit of our investments.

Can we place a value on individual countermeasures within a class?

Vaccines are the most agent specific of medical countermeasures; therefore, for agents which are rarely seen in the clinic, they have very limited application. Stockpiling vaccines for civilians makes sense for anthrax and smallpox for two reasons. For these two agents, unlike most others, vaccines can be used—in different ways—after an attack. For most other agents, efficacy of post-exposure vaccination just hasn't been demonstrated. The one instance in which, let's say a plague vaccine or an Ebola vaccine if we had one, might have utility is during a bioterrorist campaign; a series of sequential attacks (the term "reload" was coined by Secretary Danzig). Here, an individual or group attacks one U.S. city and then announces that another city will be targeted unless we capitulate. I will leave it to epidemiologists and statisticians to decide if we could respond effectively in such a situation, assuming we had the right vaccine licensed and in stock. In attempting to place a value on such a vaccine, we must consider actual cost to develop, produce and license, the shelf life, as well as the biology and the psychology involved. The behavioral and legal issues surrounding the prophylactic use of vaccines in the general population, without significant evidence of risk, can be difficult, as has been seen with both anthrax and smallpox vaccine programs in the recent past.

Antibiotics are considered a general countermeasure and, therefore, will likely have dual-utility. They can and are typically given post-exposure. This makes them ideally suited for protecting a civilian population after an attack. The issues to be considered include, first, sensitivity of the specific bacteria to a given antibiotic, then availability of the drug and its timely distribution to the affected population, if that population can be determined. Secondary issues, post attack, include possible allergy or other reactions to the drug, but the psychological and public relations issues may be slightly different after an attack than before. We currently have licensed antibiotics which are effective against most bacterial agents likely to be used by a terrorist. For some there would be issues of availability and, possibly, surge production. We believe that the Soviet Union developed antibiotic resistant strains

in the past. Resistant strains have also developed naturally' throughout the world in recent years. Although, I am not expert regarding recent submissions to the FDA, it is my understanding that there are few, if any, new classes of antibiotics moving forward for licensure. This trend should be of concern to all of us, even if there were no potential for bioterrorist attack on our population.

Anti-viral preparations can, for this purpose, be considered to have the general use characteristics of antibiotics, but are for use against viruses. They would have wide application if we never have a bioterrorist attack. For a number of reasons related to the way viruses live and function in our bodies, it is more difficult to develop antivirals that both stop the microbe and are safe for human use than it is to develop antibacterials. A very few antiviral drugs have been developed in the past 20–30 years. Now, with the availability of genomic and proteomic information, we are probably in a better position regarding the discovery or design of new classes of antivirals compounds, at least for certain families of viruses. As is with antibiotics, it is my understanding that market dynamics within the pharmaceutical industry have not, in recent years, been favorable for the development of antiviral drugs.

Antibody preparations which provide passive immune protection without vaccination, whether produced in animals, or by modern synthesis methods, have a place in our medical tool kit. They, like vaccines, are specific in that they typically are only effective against the agent they were developed for. Unlike vaccines, they can be used immediately before exposure, immediately after and in some cases in the face of disease. They are typically less effective than vaccines, even if given before exposure; an exception to this generality is the antibody preparation for botulinum toxins, which, if given before clinical signs of disease, is amazingly effective in laboratory animals. Logistically, however, antibody preparations are cumbersome in that they must be administered either intramuscularly or intravenously.

Vaccines protect by stimulating the body to produce a specific antibody which identifies and deals with the microbe when it enters the body. Antibiotics and antiviral drugs generally attack the microbe directly. There is a fourth possibility that we haven't fully exploited, primarily because we don't yet understand our immune systems well enough. This method is called non-specific immunity. Our bodies normally produce a variety of cells and chemical substances that attack microbes and help keep us healthy. These cells and chemicals deal with both bacteria and viruses. This part of our immune system is tightly integrated into our entire being and might be what we are describing when we say one person is generally "healthy" and another is not. The "innate" immune system is generally stronger when we have had a good night's sleep, when we are fit, when our nutritional and hydration status is within normal limits and when we are "happy". This protective system breaks down when we are jet-lagged or stressed. The beauty of the innate immune system is that it can protect us from many different agents and it's always on board. The limitation is that it can be easily overwhelmed. Some scientists believe that, if we could increase the "strength" of the innate immune system, we might be able to actually shift each of us toward "healthy" on the population bell curve. Today we understand this system only well enough to use very crude tools to treat some cancers and viral infections like hepatitis C. Even when we gain greater precision, it is likely that turning up the power of the innate immune system won't work for everyone. Just as a vaccine might only work for 90 percent of a given population, this method might work for 40 or 60 percent—and until we get really good, there will be significant side effects. As we learn more and more about this system, we will be better able to control it and protect humans and animals from infectious diseases. This method of protecting our citizens from biological terrorist attack—or emerging infections—may be available in 15 years—or maybe 30. It is critical that we do the basic research now to make the most of the innate immune system. This investment will pay enormous dividends even outside the world of infectious disease.

Principles regarding development of medical countermeasures for biodefense:

—Vaccines are probably the best solution, but they are good for only one microbe and must generally be given long before onset of illness. Their concept of use is more consistent with military deployment than with homeland security, with some specific exceptions.

—Antibiotics have more general application, but they are good only for bacteria.

—Antivirals that are safe and effective have been difficult to discover, but we have some new tools and should exploit them.

—Our innate immune system, if manipulated appropriately, holds promise, but we have a lot to learn before we can exploit it, especially in the healthy population.

What principles might we consider regarding acquisition of medical countermeasures?

Vaccines.—It is relatively easy to justify the acquisition of vaccines for anthrax and smallpox. Reactogenicity, cost, shelf-life, animal efficacy and licensure are all being considered. It is important that we thoroughly understand our concepts of use as we develop additional agent-specific vaccines. We should be developing next-generation flexible vaccine platforms which will allow us to relatively quickly produce and license a vaccine to counter an outbreak that subsequently becomes epidemic or pandemic. The basic platform might be licensed for use in humans, allowing us to simply add a genetic cassette when a new vaccine is needed, to greatly shorten the time to use. Our current system of vaccine research, development and approval is simply not responsive enough to respond to terrorist attack or emerging disease.

Drugs.—It is difficult to argue against spending as much as we can afford on antivirals, new classes of antibiotics and exploiting the genomic revolution to develop new categories of anti-infectives. All of these will improve the lives of Americans with or without a bioterrorist attack.

Non-Specific Therapies.—We have a long way to go to achieve broad application of what is little more than a hypothesis, but we should be doing the necessary research now. Attempting to protect our population from the unknown threat of today, and tomorrow, with specific countermeasures, will likely be extremely costly and inefficient. We probably don't yet know how much difference these preparations will make; it is likely that, for use prophylactically in the broad population where side-effects may be totally unacceptable, the value will also be minimal. In select populations or the already exposed or ill, where non-life threatening side effects are accepted, this class of drugs may be significantly more effective.

Market issues:

My experience regarding market drivers for medical countermeasures is second-hand and limited. I believe that specific countermeasures for most bioterrorism agents—and probably for emerging infectious disease—will remain in the category of orphan drugs. Research, development and production will be dependent on funding by the U.S. Government and the debate regarding licensure or investigational use will be handled for each preparation. For those countermeasures that have broader application, a significant proportion of the research will be funded by the government; however, advanced development and even production will be of interest to industry. Tax- or intellectual property-related incentives may be helpful or necessary in driving development and production, especially where the market is large enough to interest the pharmaceutical industry.

Again, I appreciate the opportunity to present this information before the Committee. I shall be happy to answer your questions.

Senator GREGG. Thank you, Dr. Franz. The last few comments there are well taken and very much appreciated. We appreciate your service to the Nation. Clearly you should have a flag painted over your front door and the appreciation should be there for all you have done in the area of protecting our soldiers, sailors, and airmen.

Dr. Read.

STATEMENT OF J. LEIGHTON READ, M.D., GENERAL PARTNER, ALLOY VENTURES

Dr. READ. Mr. Chairman and members, thank you for the opportunity to testify about BioShield and our Nation's strategy. Your interest in stopping to consider the overall approach is timely and appropriate here.

I am commenting today as an individual who has been building and financing biotechnology companies in Silicon Valley for about 17 years now. Before that I was an internal medicine doctor, and my academic career was studying costs, risks, and benefits of new medicines and vaccines.

When I received your invitation just a little a while ago, I looked up my testimony on biodefense for the Senate Governmental Affairs Committee in 2002 and then in 2003 for the Subcommittees

of the House Energy and Commerce Committee. Re-reading that testimony, I have to say I had concerns and recommendations that I voiced then that are just as relevant today as they were when the Department of Homeland Security and Project BioShield were still on the drawing board. So there is clearly still some work to do.

This problem requires long-term thinking. I agree with statements made earlier by your colleagues that there is no potential threat to us. I would like to focus particularly on our economy and our lifestyle. If an easy-to-deploy, transmissible bioweapon were deployed, even with a very small loss of life, the impact on our economy would be unbelievable because the necessary steps to interrupt the chain of transmission would interfere with travel and commerce of all kinds, even potentially food and medical supply distribution. Most importantly, I am really concerned about the impact of this on the freedom of people to meet during a time of stress and worry and political consequence. Nothing would test our trust in Government authority more than a quarantine separating loved ones. So, the stakes are very high.

One of the companies I built was in the influenza vaccine business, and I agree it would be a very realistic proposition that someone could smuggle a dangerous strain of influenza into the United States. That deserves serious attention.

Now, a great deal of positive work has been done. It is hard to describe how big a step forward the BioShield legislation was and some of the implementation that has followed that at the same time as talking about how much is still to be done, but we need to do that. Much remains to be done to educate the public and strengthen our traditional public health systems, our first responders.

I was very heartened by some of the responses to the presidential directives in Mr. Albright's testimony. Many of those problems or challenges can be dealt with in just a few years of sustained effort, and one of my key points is that is not the case for our longest lead time countermeasures, drugs and vaccines, that have not even been invented yet to counter these threats. As you know, drugs typically take 5 to 10 years from the first commitment to do something to the delivery of something for patients; vaccines, more like 10 to 20 years.

This company I founded in 1992 licensed a very promising influenza vaccine, nasal influenza vaccine technology from the University of Michigan in 1995. This technology had already undergone 20 years of clinical trials under NIH support, and yet it was 2003, 8 years later, and after the expenditure of $1 billion by three different companies of private capital before this product was approved by the FDA. This is a product known as FluMist which is now of growing importance as part of our influenza protection armamentarium.

My second point is we clearly need the private sector to be involved and BioShield represented a very strong and clear recognition that this was the case, that we needed to get the incentives right. There are many reasons why we need the private sector, but basically all of the drugs and vaccines we use today for everything outside the field of biodefense come from the private sector, admit-

tedly and with great respect for the huge national investment in the basic science made these discoveries possible.

Start-ups and smaller companies play a very important role. I invest in these companies as a full-time venture capitalist. They take on higher-risk projects. They can demonstrate proof of principle.

But I would like to underscore today the importance of the larger, more capable companies. They often acquire technology by acquiring these smaller companies that we invest in or by carrying out licensing deals with them. But there are skills for the downstream development of pharmaceuticals and vaccines that are very hard to come by outside a relatively small number of very large pharmaceutical and biotechnology companies. The real test of whether BioShield is working is whether it engages the capabilities of these companies in the development of countermeasures. I would say we are not there yet.

A biodefense procurement strategy that relies on companies that have not even launched a commercial product is likely to incur extra delays and other down-side surprises. So this is really a point for attention.

What I think is a key missing ingredient is, we need markets for these products which mimic the size and the predictability of markets for treatment and prevention of other diseases. That is really the goal. The current BioShield law was, as I said, a step in the right direction, but it fails to adequately signal the Government's intention to purchase successful countermeasures. We need much more transparency on what the priority list is so the companies can begin to think about these things in advance. We need much more clarity about who are the people who have both the knowledge to comment and the authority to make decisions.

There are lessons to be learned from some of the ideas being aggressively explored to stimulate private sector investment in vaccines for global health problems, such as AIDS, malaria, and TB. This notion of advanced purchase contracts deserves study as a model for your continued refinement and enhancement of BioShield. The notion there is a strong connection between the benefits of investing in infectious disease research for other diseases or even broadly and defense against biodefense is a very valid concept that is completely appropriate.

BioShield misses in important respects with respect to providing indemnification from product liability. Basically it is a test of confidence. If a company tells you they are not really concerned about that in a conversation about working with the Government in biodefense, it is just because they have not grown up to understand how critical it is for their shareholders.

We need to streamline procurement. It is not clear that any of the work so far by our great public servants who are carrying out the legislation of BioShield have taken advantage of the full ability to streamline the procurement process and take advantage of those special provisions. I think that is going to be important.

I would like to come back to emphasize the point raised by Senator Stevens that we need a way to screen. As a venture capitalist, we get a very large number of proposals for investments, and only a tiny, tiny percentage are actually companies that receive investment. We have worked out screening processes, and I do not know

that it is a model but it makes me sympathetic to the problem of a public servant who gets calls from people who think they have a good idea but the science is not really there and the person who gets lost in that crowd really does have the right idea. I can think of a number of ways we could use some of the new technologies, web-based technologies, table top exercises and maybe even a private sector intermediary to help with some of the filtering.

We are in a biological arms race with our future attackers, and there are specific targets we should be going after. I completely agree with the priority for anthrax and smallpox. That makes sense to me. I must say it is pretty hard for people outside the Government to figure out what the priority list is below that. We have the long list of 20 or 30 agents, but the Government's own thinking about the rank order of what comes after smallpox and anthrax for civilians in particular is obscure. And it seems to me while it might require some defense of that ranking and that might be a little bit difficult, that it should be transparent so the private sector can set priorities.

Sooner or later, despite our efforts to make good specific countermeasures, a clever or lucky perpetrator may deploy an agent for which we have not made specific preparations. And this calls for the notion of some kind of broader approach. We may need broad spectrum antimicrobials or vaccines, as has been mentioned. We may need to harness the nonspecific defenses already working in human biology like innate immunity. We may need to build systems, still very speculative, that you could move from obtaining the pathogen to having a drug in a very short time period. And all of those are worth stimulating some kind of prize or novel recognition and financial reward for some of these more speculative approaches. It might be very useful. I compare it to the X-prize for manned space flight that was successfully competed for and won in the last year.

If we want to think about this broadly and in the long time frame which is really appropriate, a 2030, maybe even longer time horizon, we should be looking broadly. One idea I would like to suggest as an example, it should be studied before moving forward, would be to think about a survey of the microbial world on a scale that has not been attempted. Just as we carry out ambitious projects to systematically catalog the sky within reach of our light and radio telescopes, maybe it is time to carry out a planetary scale survey of humans and the microorganisms with which we frequently interact. We might want to begin by focusing on the respiratory tract.

PREPARED STATEMENT

There is technology available. I cite a remarkable experiment by Craig Venter's group in which they obtained sequences for over a million new genes by looking at 1,500 liters of Atlantic seawater. A company called Affy Metrix has gene chips that have been used to study which organisms are present in nasal swabs taken from approximately 10,000 subjects in studies. So it is possible now with some of the technology to think about such a broad survey. Not only could it provide us a baseline for measurement of new emerging infections by intent or by nature, but the basic science that

would be enabled by this survey could provide more fundamental understandings to help us deal with the general problem.

Thank you very much, Mr. Chairman.

[The statement follows:]

PREPARED STATEMENT OF J. LEIGHTON READ, M.D.

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today regarding BioShield and our Nation's strategy for confronting bioterrorism. Your interest in stopping to consider our overall approach is timely and appropriate.

I am commenting today as an individual who has been building and financing biotechnology companies in Silicon Valley for over 17 years. Before that, I was an internal medicine doctor doing research on the cost, risk and benefits of new medicines and vaccines. On receiving your invitation to appear here, I looked up my testimony on biodefense for the Senate Governmental Affairs Committee [1] in 2002 and for Subcommittees of the House Energy and Commerce Committee [2] in 2003.

Unfortunately, the concerns and recommendations voiced then are as just as relevant today as they were when the Department of Homeland Security and Project BioShield were still on the drawing board. Since those remarks are available on the internet, I will only restate the main points here before turning to new thoughts.

Long Term Thinking

Biodefense is a gigantic, long-term problem. There is no potential threat to our economy or lifestyle that would be as easy to deploy or costly to contain as the release of a transmissible bioweapon. We should be clear that deliberate introduction of an agent that spreads from person to person is a completely different category of risk than an attack with dangerous organisms that do not spread. This is because our reasonable efforts to interrupt the chain of transmission would interfere with travel and commerce of all kinds, including distribution of food and medical supplies, and importantly, the freedom for people to meet each other in a time of grave worry and political consequence. Effective quarantine separating loved ones will profoundly test our trust in government authority.

Despite a great deal of positive work, we are not yet organized to deal with this threat. Much remains to be done in educating the public and strengthening traditional public health systems and our first responders. Fortunately, much of this kind of work can be accomplished in only a few years of sustained effort. That is not the case for the longest lead-time components of our readiness: medicines, vaccines and other biomedical technologies needed to protect our population and that of our trading partners. For drugs against viruses or bacteria, it takes 5–10 years from commitment to delivery of medicine for patients. The process for vaccines typically takes 10–20 years. In 1995, a company I founded, named Aviron, licensed a promising intranasal influenza vaccine from the University of Michigan that had already undergone 20 years of clinical testing by the NIH. It took nine more years and over $1 billion in private investment by three companies before the product known as FluMist™ was approved by the FDA. Despite these timelines and costs, some pathogens are such natural candidates for potential abuse well into the foreseeable future that we must begin work now. It is important to seize this opportunity because infectious diseases represent some of our greatest triumphs in discovering, preventing and treating disease.

Larger, More Capable Companies must be Involved

This work will require enthusiastic and committed engagement by our country's most capable pharmaceutical and biotechnology companies. All of the drugs and vaccines in use in the United States come from the private sector, often after substantial public investment in government and university laboratories. Start-ups and smaller companies play an essential role in taking on many higher-risk projects and demonstrating proof of principle. Larger players gain access to these technologies through licensing deals or purchase of the smaller companies. Several hundred million dollars of private capital and down-stream development skills rarely found outside of larger companies are usually required to finish the job for each important innovation. When R&D is successful, this investment makes sense because innovative products that address substantial medical need are reimbursed at the high value they represent to patients and healthcare payers.

[1] http://www.bens.org/highlights_testimony_read.html.
[2] http://www.bio.org/healthcare/biodefense/20030327.asp.

The experience factor is so important that a biodefense procurement strategy that relies on companies with scant experience in launching commercial products is likely to incur extra delays and other down-side surprises. Yet this appears to be exactly where we are heading with BioShield because the market incentives are not yet in place to attract the most capable innovators.

The missing ingredients for biodefense countermeasures are markets which mimic the size and predictability of markets for treatment and prevention of other serious diseases. The current BioShield law provided an important step in the right direction, but it fails to adequately signal the Government's intention to purchase successful countermeasures that are still years away from completion. There is much to be learned from progress in defining Advanced Purchase Contracts and related "pull" mechanisms for stimulating vaccine R&D against global health targets such as malaria., tuberculosis and HIV. Restoration of patent term lost during regulatory review will be helpful. Important gaps still remain in the details and degree of indemnification from product liability. Larger, more capable companies will not participate unless these problems are addressed in future legislation.

Streamline Procurement and Improve the Dialogue With Industry

It is time to finish the job of re-inventing procurement of biodefense countermeasures. The bureaucratic tangle of approvals and sign-offs involving multiple agencies and departments (even including the President) prescribed in BioShield must be streamlined. Spending authority should be concentrated in the hands of someone close to the intelligence analysis which helps set priorities.

It is essential that much more frequent and transparent conversation occur between companies and those setting the priorities for countermeasures. The formal process of RFPs and related acronyms cannot substitute for frequent, informal contact. Novel formats for meetings, including more table-top exercises web-based interactions should be encouraged. Antitrust relief may be required if these concerns are inhibiting valuable multiparty conversations.

BioShield did not adequately address the need for more centralization of authority for setting priorities, funding solutions, and managing incentives. There is a recurring theme in my conversations with executives interested in making a contribution to biodefense: they can't find the right person in the government who knows the issues AND can make a decision. This more centralized authority should also have enhanced ability to adjust FDA influence processes and safety standards in preparing for high-risk threats.

A Biological Arms Race

One can identify the highest risk agents for the near and intermediate time frame, based on the biology of the microbes, the technical challenges faced by our potential attackers and intelligence data. These agents are presumably at the top of the priority list for BioShield, although it is hard to get clarity about which of a dozen potential threats rank most highly after anthrax and smallpox. There are at least a dozen agents that deserve serious countermeasure investment.

Sooner or later, however, a clever or lucky perpetrator may deploy an agent for which we have not make specific preparations. It may have been derived from nature, cultivated in the laboratory, or engineered to have novel drug resistance or host range. There are several paths to get ready for this event. One is to seek broader spectrum antimicrobial drugs or vaccines. While there are examples of such agents discovered by accident, the rational design of broad spectrum countermeasures is largely beyond our current capabilities. Another path is to harness and enhance the non-specific defenses already available in human biology. We are still early in our understanding of how to manipulate innate immunity and the role of cellular factors such as interferon. Finally, highly speculative processes have been proposed by which one could move from knowledge of a new pathogen to a new treatment in a month, or a week, or a day. Technologies such as antisense agents and interfering RNAs may hold promise for such a goal.

Our biodefense strategy must include a mix of disease-specific countermeasures and new technologies which offer more general treatment or prevention. I am concerned that getting the right mix depends on the quality of the dialogue among companies and the diverse government agencies that are involved. A high level of transparency on priorities and authority will be essential before the parties can effectively explore technical risk and financial incentives needed to get the job done. For some of the more aggressive goals, serious prizes, such as the X-prize for manned space flight may be the most appropriate way to focus innovator's attention.

The Basic Science of Biodefense

Our country has made and continues to make a large national investment in the underlying science of infectious disease and host defense. This effort is serving us

well in many current biodefense efforts. In many cases, adequate financial rewards for the final product will provide incentives to develop new research tools along the way. In other cases, and particularly, animal models it is more efficient to have centralized research tools that can be shared by many innovators. When the government has the keys to scarce resources needed to carry out research, such as higher level biocontainment facilities, or access to dangerous strains, it is essential that access be facilitated for all who need them in pursuit of sanctioned goals.

It may be time to consider an even bolder investment in basic understanding of the relationship between humans and microbes. Research is giving us a growing appreciation of the interdependency of genetics and environment, with particular emphasis on the environmental interaction of unrelated, but physically proximal organisms. Technology is now available to conduct a broad survey of microorganism diversity, genetics and metabolism A few projects have demonstrated the feasibility of collecting and analyzing data on a very large number of organisms. One example is Craig Venter's report on a rapid genetic sequencing technique that found evidence of 1.2 million new genes in 1,500 liters of Atlantic seawater. Another comes from a company called Affymetrix whose gene chips have been used to identify which organisms are present in nasal swabs taken from thousands of study subjects.

Just as we have carried out ambitious projects to systematically catalogue all of the heavenly bodies within reach of our telescopes, it may be time to carry out a planetary-scale survey of humans and the microorganisms with which they frequently interact. A focus on agents which colonize or infect the respiratory track might be the best place to begin. Data from such a survey could serve as a baseline for detecting introduction of novel threats. More importantly, analysis of the data could lead to more fundamental understanding of how to create robust protection against such threats.

Mr. Chairman, I know that you have recently introduced legislation that would address many of the concerns mentioned here. Thank you for your leadership on this issue and your persistence in asking whether we are doing enough of the right things at the right time. I would be happy to provide further comment if you have questions.

Senator GREGG. Thank you.

I have to recess. I have got to make a quick phone call. I will be right back. It should not take more than 5 minutes.

Thank you for your courtesy. I apologize for the interruption.

Mr. Clerici.

STATEMENT OF JOHN M. CLERICI, ESQ., PARTNER, McKENNA, LONG & ALDRIDGE, LLP

Mr. CLERICI. Thank you, Mr. Chairman. Mr. Chairman, members of this subcommittee, it is an honor to testify before you regarding my views of where we are with Project BioShield and biodefense in general. I applaud the leadership of you, Mr. Chairman Gregg, in your work on the Health Committee and being the lead sponsor on BioShield I, and also applaud the bipartisan leadership of Senator Lieberman and Senator Hatch, and Senator Kennedy, obviously, took a great leadership role in that effort and continue to be leaders on the issue of biodefense.

Over the last few years, I have had the chance to personally work with the Department of Health and Human Services on behalf of a number of clients and entities not only in the area of biodefense, but also emerging infectious disease. We have negotiated contracts, some of which Assistant Secretary Simonson referred to, for SARS, avian flu, pandemic influenza planning, and other issues.

Based upon that experience, it is clear to me that HHS does need additional tools beyond what was provided in BioShield to get the goals accomplished that the legislation meant to accomplish. Primary and first among those goals, as Dr. Read has pointed out, is to address the issue of liability.

As we have begun to purchase these countermeasures slowly and there have been a couple contracts let to date, as Assistant Secretary Simonson said, and a few more on the way shortly, the primary obstacle at the end of the day to getting these deals done is addressing how liability concerns will be addressed. Certainly, as Dr. Read just pointed out, the liability concerns of a public company with shareholders and large assets are much different than a small biotech which has the ability to bet the company without worrying about liability. And I am not sure those are the types of companies we want necessarily participating or leading the way in this effort to bring these countermeasures to market.

Today, there are two primary ways liability can be addressed. Public Law 85–804 has been on the books since the first Wars Powers Act during World War II, and it allows the Government to indemnify contractors after award, only after award, for risks that are deemed in the national security interest. It is an indemnity contract. Therefore, the public is at risk, and I know in your role as budget chairman is of great concern to you as well, Senator. But unfortunately, it provides no predictability because you do not know whether you are going to get liability protection until after you bid on the proposal, negotiated a contract, and are prepared to deliver. It provides no certainty to industry and no transparency to industry to plan.

The second mechanism has been pointed to is the SAFETY Act, and I am very familiar with the operations of the SAFETY Act. It is a piece of landmark legislation to address the tort concerns of providers of Homeland Security goods and services in general. It does not work particularly well for countermeasures for two primary reasons.

First, the SAFETY Act has a gap in it that does not protect vaccine manufacturers because the liabilities removed by the SAFETY Act are only those that occur following an act of terrorism. Most of the liability concerns of a vaccine manufacturer are, of course, before anything has happened. It is in the administration of the vaccine itself.

Second, much like with Public Law 85–804, it is an application process, and there is lack of predictability involved with the SAFETY Act. And currently there are less than 20 companies that have been certified under the Act and no biodefense measures or pharmaceutical companies are among those.

The SAFETY Act also requires a company to litigate all over the country to exert what amounts to an affirmative defense to get out of litigation. Therefore, there are still substantial uncertainty subject to the judicial system in America, which is obviously not something that anyone wants to be their company on sometimes.

I note in your bill, Senator, in Senate bill 3, you have done an excellent job of addressing, in my view, the liability concerns for biodefense manufacturers, and you also attempt to address the liability concerns of pandemic flu manufacturers. As we heard during the previous panel, the threat facing the country from a pandemic flu is much greater in my mind than the threat facing the country in bioterrorism, and that threat is enormous, as you know. The 1918 influenza pandemic, Spanish flu pandemic, killed millions of Americans, and unless we are prepared for that pandemic,

we will be facing those same sort of liabilities both in terms of lives and in dollars if another influenza pandemic occurs again.

The reason why pandemic influenza should be treated off line in my view is the sense of urgency. No amount of detection, no amount of intervention, and we can have the biggest armies and navies in the world, are going to prevent mother nature from affecting us. And this is urgent. We are past the time when this country and this world should be facing a pandemic based on statistics.

The threat of pandemic liability is much like the threat of smallpox in the sense that if there is a pandemic, you will need to vaccinate the entire Nation. And your previous committee, the Health Committee, and through the Homeland Security Act, addressed the liability for smallpox vaccine manufacturers particularly by providing them immunity. We need to provide at least the same sense of liability protection to providers of pandemic flu vaccine because the threat from liability is identical, if not greater than the threat of liability from a smallpox vaccine manufacturer.

Your staff has also asked me, Senator, to address some of the challenges in the implementation of the procurement provisions of BioShield, aside from liability, and liability is certainly first among them again.

As Dr. Read has mentioned, the Department, in implementing Project BioShield, has not taken full advantage of all of the authorities that Project BioShield gave them back in 2004 when the legislation was signed. They have the ability at HHS to conduct these procurements under simplified acquisition rules. They have not exercised that authority to date. What has transpired through these negotiations is nongovernmental contractors, commercial entities, that are not used to doing business with the Federal Government are subject to the same amount of Federal acquisition regulation that our large defense contractors are subject to in providing these goods and services. That causes them both delay, uncertainty, a lack of transparency in what they are signing up to, and the delays resulted have been definitely inhibiting our ability to bring these countermeasures into the market as quickly as possible.

We have discussed already there have been two awards to date, primarily big awards. There is a third smaller award addressing irradiation treatment for children, but two large awards using the special reserve fund under Project BioShield, one large award and one RFP pending, one award pending.

The first award went to VaxGen which has already been discussed. Although that is often labeled as the first BioShield procurement, I would disagree with that characterization. It is the first procurement using BioShield funding, but the mechanisms to procure that countermeasure was done the same traditional way the Government would normally procure things. It was a multistage procurement, taxpayer-funded research and development resulting in, at the end of the day, a contract that as Secretary Simonson says, will not be paid until substantial delivery but, nevertheless, is a multi-stage, prolonged procurement. We did not set a market or set someone to guarantee it. Rather we had them chase the market just as if they would traditionally.

The next award up in Project BioShield will most likely be for anthrax therapeutic, and Secretary Simonson mentioned that as well. Now, that will be the very first BioShield procurement, but again, HHS has not made use, in the solicitation at least, of the simplified acquisition procedures allowed to make use of it during that process.

As a result, those contractors, whoever will get this award, face the possibility of very powerful and strong regulatory burdens upon them, including certified cost and pricing data and other burdens that have led this award to take over a year at this point from award. The request for information for anthrax therapeutics was issued on April 1, 2004, and I believe we are at least 2 months away from award for that contract. So these pharmaceuticals and these vaccines are not entering the stockpile at the rate I think Congress intended.

PREPARED STATEMENTS

Going forward, we can certainly do oversight to make sure that HHS and DHS work closely together to make better use of the authorities that BioShield I provided them. We can also, through BioShield II or other legislation such as Senate bill S. 3, provide additional tools such as liability reform and encouragement to make clear these contracts are not to be burden by over-regulation.

I look forward to your questions. Thank you very much.

[The statements follow:]

PREPARED STATEMENT OF JOHN M. CLERICI

Chairman Gregg, Senator Byrd, and Members of the Committee, it is an honor for me to testify before you today regarding my views on the Project Bioshield Act of 2004 and whether we are meeting the biodefense needs of the United States.

I appear before you today as someone who has worked with industries helping to supply the United States with critical biodefense, chemical, radiological, and nuclear countermeasures since even before the attacks of 2001. During this time, I have worked with a number of large pharmaceutical companies, mid and small size biotechs, and companies that provide detection equipment and other ancillary services to help protect the Nation from the threat of biological, chemical, nuclear, or radiological weapons. I also have had the opportunity to work with Congress and the Administration to help formulate policies to stimulate the creation of a thriving bio-defense industry in America. I and other members of our firm have provided testimony to both the House and Senate regarding the Project Bioshield Act of 2004 and we continue to work closely with your staff, Mr. Chairman, and the staff of other leaders in this area, including Senator Lieberman, Senator Kennedy, Senator Burr, and Senator Enzi, to ensure the best possible policies are in place to promote the deployment of the best possible countermeasures in this critical area.

During the last 3 years, I have been personally involved with a number of direct negotiations with the Department of Health and Human Services (HHS) for a number of critical biodefense countermeasures, as well as negotiations for contracts for critical vaccines for emerging infectious disease such as SARS, Avian influenza, and pandemic influenza. That said, it is my view, and I believe the view of many others in this industry, that HHS should be given additional tools to maximize participation of the entities that are best suited to provide critical countermeasures.

First among these additional tools must be expanded authority to address the issue of unmitigated liability associated with undertaking Bioshield contracts.

Liability Must be Addressed to Have a Successful Bio-Defense Industry

Industry concerns over the massive cost of product liability lawsuits are preventing critical countermeasures from being developed for the Strategic National Stockpile (SNS). The liability concerns of a company engaged in day-to-day drug development are clearly different from the liability concerns of a company participating in Project Bioshield. Manufacturers of countermeasures produced under Project Bioshield risk exposure to devastating product liability lawsuits to a far

greater degree than typical drug companies. Safety and efficacy data must be derived, for the most part, from animal trials since healthy humans cannot be exposed to toxic agents during testing. Thus, these critical countermeasures must be developed and are likely to be deployed without the full battery of testing typical of other drugs. Without liability protections, responsible companies will remain on the sidelines for fear of risking corporate assets to defend lawsuits brought as a result of producing a countermeasure that generally has a much lower profit margin than a typical pharmaceutical product.

Even as the Federal Government has begun to purchase Bioshield countermeasures, it has no current way to resolve issues of liability with any degree of certainty. As a result, needed countermeasures are not being developed and deployed, thereby exposing the economy, and the Nation as a whole, to far greater potential liability due to the lack of available effective countermeasures in the event of attack. Either way, the Federal Government is likely to bear both the human and financial cost of such an attack as it did on September 11th. By failing to account for these costs before an attack, countermeasures will not be developed and the Nation will be more exposed to attack.

Senate Bill 3 attempts to address these liability concerns for not only terrorism, but also countermeasures developed and deployed to protect the United States against naturally occurring epidemics such as SARS and pandemics such as Avian influenza. These epidemics and pandemics have the potential to be even more costly in terms of lives and dollars than even the worst terrorist attack. By addressing the issue of liability before an event occurs, we are not only assuring that needed countermeasures are developed, but also, being fiscally responsible by mitigating at the least economic cost of such a tragedy and reducing the cost of needless litigation.

While the similarities between the public health threats of bio-defense and infectious disease are obvious, I would strongly urge Congress to consider—and act upon—liability protections that are necessary to bring a pandemic influenza vaccine to market as quickly as possible. The dangers of a pandemic are real and immediate. Should the Nation face a pandemic similar to the one it faced in 1918 and 1919 with the Spanish flu, millions of American are certain to die. While I do believe Senate Bill 3 provides adequate protections to stimulate the creation of a bio-defense industry, it is inadequate to protect providers of pandemic vaccine given that the response to such an event would be to quickly vaccinate nearly 300 million Americans. Thus, the response to a pandemic is similar to—and perhaps, far broader than—the response to a potential outbreak of smallpox. For this reason, the liability protections provided for a pandemic influenza vaccine provider must be at least as strong as those protections given to providers of smallpox vaccine under the Homeland Security Act of 2002.

Under the Homeland Security Act of 2002, manufactures, suppliers and administrators of smallpox vaccine are immune from any and all liability resulting from the administration of the vaccine during a declared emergency. These protections provide the certainty necessary to ensure the Nation has an adequate supply of smallpox vaccine in the event of an attack. While there are several improvements that should be made to this legislation to ensure health care workers are properly compensated, these same types of protections must be extended to providers of pandemic influenza vaccine.

Available Liability Mitigation Tools are Inadequate

Under current law, there are currently only two legal authorities that allow the Federal Government to mitigate the liability concerns for providers of countermeasures other than smallpox vaccine—through Federal indemnification under Public Law 85–804 and through designation/certification under the SAFETY Act. Both measures are inadequate to address the practical realities of potential litigation facing the providers of countermeasures and the fiscal realities facing the Federal Government

Public Law 85–804 grants the President an extremely broad authority to allow a Federal Government contractor to obtain financial or other forms of relief under certain circumstances, even when the government may have no express legal obligation to grant such relief, or when there are express prohibitions against such relief contained in other statutes, regulations, or common law. Under this authority, the heads of designated departments or agencies have the discretionary power to provide contractors with government indemnity when they are engaged in "unusually hazardous" activities and when it is in the interest of the national defense to provide such indemnity.

Indemnification under Public Law 85–804 relies upon the American tort system and places the Federal Government in the position of an insurer—where payments are made only after all claims have been adjudicated in the court system and judg-

ments have been rendered. This rather lengthy process does not result in compensation to victims being paid in a timely manner nor does it place any effective limits on the Federal Government's potential payments to victims when it acts in this capacity.

Although this authority has been invoked by the Department of Health and Human Services (which was first granted the authority in October 2001 following the anthrax attacks) in agreements involving the donation of smallpox vaccine by Wyeth and Aventis Pasteur to the Federal Government in 2001, HHS will only address the issue of indemnification prior to the award of a contract for a countermeasure. As a result, potential providers of countermeasures must expend scarce resources to prepare and submit a proposal that may result in a contract that cannot be accepted due to the lack of liability protections should HHS ultimately refuse to provide indemnification. More often, companies simply refuse to bid at all due to the lack of certainty on the issue of liability. This has resulted in the largest, and far more experienced, drug companies with the necessary expertise to address this threat being left on the sidelines.

Moreover, HHS and OMB have taken the position that indemnification under Public Law 85–804 cannot be granted to protect suppliers of pandemic influenza vaccine since there is not an immediate connection to national security. This extremely narrow view of what constitutes "national security" ignores the implications that our troops stationed in Southwest Asia (which is currently facing a potential Avian Flu epidemic), it also ignores the national security implications of having millions of America perish in a pandemic. Thus, Congress must address this issue immediately to ensure the Nation is fully prepared.

Congress did attempt to address the issue of liability associated with antiterrorism goods and services with the passage of the SAFETY Act in November 2002. The SAFETY Act does, in fact, provide significant protections to providers of countermeasures that receive certification under the Act. However, to date, no such certifications have been granted for bio-defense countermeasures. In addition, there are specific limitations upon the effectiveness of the SAFETY Act for providers of countermeasures under Project Bioshield.

Section 865(1) of the SAFETY Act notes that qualified anti-terrorism technologies may include technologies deployed for the purpose of "limiting the harm such acts [of terrorism] might otherwise cause." The "harm" that may be caused by an act of terrorism clearly goes beyond the immediate effects of the Act itself. An act of terrorism such as the attacks of September 11th or the October 2001 anthrax attacks trigger a number of immediate remedial and emergency responses to limit the resulting harm and deter follow-on attacks.

While the SAFETY Act can provide signification protections to a company, its application in the context of countermeasures is extremely limited. Most significantly, the potential liability of a provider of anti-terrorist technologies that may allegedly cause injury PRIOR to a terrorist attack, such as a vaccine, are not currently addressed by the SAFETY Act. This limitation of the SAFETY Act leaves providers of anti-terrorism vaccines without any adequate projections aside from the possibility of Federal indemnification.

Moreover, SAFETY Act certification is most inadequate to provide the type of protections required for large companies to enter the market for countermeasures. Holders of SAFETY Act certification are still faced with the possibility of hundreds of lawsuits brought against them throughout the country, albeit in Federal court. Since the SAFETY Act protections must be asserted as an affirmative defense to any lawsuit, the unpredictability of the American judicial system still places providers of countermeasures with a large degree of uncertainty regarding potential liability. This uncertainty, coupled with the "gap" in the SAFETY Act for vaccine providers and the cumbersome nature of the application process to receive SAFETY Act certification makes it an inadequate protection for providers of countermeasures under Project Bioshield.

For all of these reasons, Congress should equip HHS with the adequate tools to address liability concerns that are inhibiting the development and deployment of critical countermeasures as soon as possible. More over, it is in the best interests of the United States that Congress act immediately to extend the same types of protections afforded to providers of smallpox vaccine to providers of pandemic influenza vaccine to ensure an adequate response to the certain public health crisis an influenza pandemic will cause the United States unless we are adequately prepared.

Additional Regulatory Relief for Providers of Countermeasures is Needed

The Project Bioshield Act of 2004 makes great strides to reduce many of the regulatory burdens that are obstacles to allowing companies that do not traditionally sell the Federal Government to participate in the development of needed counter-

measures. Based upon the experience of industry during the first procurements conducted Bioshield, more can be done to reduce the amount unnecessarily burdensome regulations. To date, industry reaction to Bioshield has been muted, partly because of initial implementation challenges and partly because the scope and incentives of Bioshield are too limited to attract serious attention from investors, including venture capitalists, institutional investors, or manufacturers that are needed to grow the biodefense industry.

It is important to examine the first actions HHS has taken under the Project Bioshield to understand the challenges in implementing the statute, as well as the need for additional procurement reforms.

On October 26, 2004, HHS received the first proposals to provide therapeutic products for treatment of inhalational anthrax disease in response to Solicitation No. 2004–N–01385 (the "Anthrax Therapeutics Solicitation") under what was the first, true, Project Bioshield procurement. Just over 2 weeks later, on November 4, 2004, VaxGen, Inc. ("VaxGen") received an award of a large contract to produce an experimental recombinant protective antigen anthrax vaccine ("rPA").

While this award to VaxGen was the first countermeasure contract funded from Bioshield's Special Reserve Fund, this was not a true Bioshield procurement. In fact, all of the research and development for this countermeasure was funded at the taxpayer's expense through the National Institute for Allergy and Infectious Disease under two earlier awards totaling over $200 million. Unlike the goals of Bioshield to create a market to encourage private investment, the first award funded by Bioshield was a very typical, multi-stage, Federal procurement fully funded at the taxpayer's expense, without utilizing any of the unique authorities Congress provided to HHS under Project Bioshield.

The first Bioshield procurement for Anthrax therapeutics solicitation is for the acquisition and maintenance within the SNS of therapeutic products to treat U.S. civilians who have inhalational anthrax disease. The Anthrax therapeutics solicitation contemplates that the awarded contract(s) will be for 10 grams of an investigational new drug ("IND") for use in testing. The actual manufacture of anthrax therapeutic product is an optional contract line item, which the government may decide to exercise within 12 months from the date of contract award and after the government reviews and approves the test sample. However, while this procurement could have utilized the streamlined procurement provisions provided under Project Bioshield, the solicitation includes numerous provisions of the Federal Acquisition Regulation ("FAR") and other detailed requirements for bidders, including detailed rules governing the methods of preparing pricing for the proposal.

This initial Bioshield solicitation was curious in three ways. First, the way the solicitation structures the options in the contract fall short of the Congressional intent of the Act to provide for a commitment to recommend funding for production for the SNS as contemplated by Project Bioshield. Contrary to the intent of the Act, HHS has not committed to recommend exercise of the options for production quantities of the countermeasure upon successful development of the countermeasure. Such a commitment would help to advance the Act's purpose of promoting the development of a biodefense industry by informing the markets that there is some certainty that there will be a government market for the product. Second, as noted above, the solicitation failed to use the simplified acquisition authorities that Bioshield makes available to the government, which would have permitted far fewer bidding requirements. Third, the solicitation makes IND status an absolute criteria for award of the contract. This has been criticized as unduly—restricting the ability of companies with promising technologies that have not yet reached IND, FDP status from competing.

Unlike the Anthrax therapeutics solicitation, the VaxGen solicitation did not suffer from a lack of commitment to production quantities. The scope of work for the rPA contract requires VaxGen to manufacture and deliver to the SNS 75 million doses of experimental (and non-FDA approved) rPA vaccine in pre-filled syringes along with safety needles (with a minimum of 25 million doses delivered within two years of contract award). The contract also requires a variety of ancillary commitments by VaxGen related to testing and licensing.

The VaxGen contract is valued at $877.5 million, representing approximately 15 percent of the amounts appropriated for Project Bioshield for the next 10 years. The contract provides for payments to VaxGen of $754 million in advance of the following milestones: (1) approval of a Biologics License Application ("BLA") for general use prophylaxis, (2) approval of a BLA for post exposure prophylaxis; and (3) demonstration of 18 months of real time stability in pre-filled syringes. When and if these milestones are accomplished, VaxGen will receive specified per dose price supplements.

There are three main criticisms of the VaxGen contract. First, it appears that, as with the Anthrax therapeutics solicitation, HHS elected not to use simplified acquisition procedures in awarding the contract. Second, despite the availability of an FDA licensed competing vaccine technology, HHS restricted the competition for the contract to firms that produced rPA-based vaccines, which have not been advanced beyond early testing in the regulatory approval process. This has made the government and the Nation's security against anthrax attacks highly dependent on an early stage, unproven technology. Third, the government awarded the contract to a single vendor, thereby making the Nation's security against such attacks dependent on this single vendor.

Proposed Implementation Improvements

HHS can take several steps to implement Bioshield to increase industry participation. To fully realize the legislative intent of the law, HHS should enact regulations required under the Project Bioshield Act that take into account the following issues:

—Specify that Project Bioshield Act procurements include only those FAR clauses specifically required by FAR Part 13, Simplified Acquisition Procedures;

—Fully describe how HHS and DHS will make a determination of a material threat and the other determinations required by the Project Bioshield Act;

—Provide for determinations of the order in which the government plans to procure countermeasures;

—Require HHS to specify a firm number of doses or courses of treatment in the call for countermeasures stage;

—Provide for industry participation in market surveys undertaken during the assessment of the availability and appropriateness of countermeasures stage;

—Provide critical suppliers of needed medical countermeasures annual "warm base" funding to ensure that the U.S. Government will have continued access to those products following any procurement contract;

—Provide that multiple products manufactured by multiple suppliers using multiple technologies be procured where practicable to avoid undue dependence on any single supplier or single technology;

—Provide that countermeasures that are already licensed by the Food and Drug Administration should where possible be purchased under Project Bioshield; and

—Provide for the appropriate use of HHS' "Other Transaction" Authority in procurements under Sections 2 and 3 of the Project Bioshield Act, in accordance with the authority provided to HHS by Title XVI of the fiscal year 2004 Defense Authorization Act.

Also, as required by Section 319F–2(c)(4)(C)(ii) of the Public Health Act, HHS should, in a call for bio-terrorism countermeasures, provide industry with an estimate of the quantities of a countermeasure (in the form of number of doses or number of effective courses of treatment) that HHS intends to procure upon development of a countermeasure that meets the statutory criteria. Providing industry with wide ranges of potential requirements for a countermeasure, as HHS did in the Anthrax therapeutics solicitation, does not serve the statutory purpose of promoting the development of a biodefense industry because it introduces additional uncertainty about the size of the government market for the countermeasure.

HHS and the Department of Homeland Security ("DHS") should provide industry with information concerning the implementation of the Project Bioshield Act. For example, HHS and DHS should provide industry and the public with a status report concerning the governmental processes required by Section 319F–2(c)(2)–(6) of the Public Health Act. HHS should also publish the report on the adequacy of biocontainment facilities required by Sec. 5(c) of the Project Bioshield Act. This report was due in January, and yet, has not been completed or provided to industry.

Perhaps most important, DHS should inform industry of the progress and priority of the required threat assessments so that companies can make proper business decisions in their planning process. Project Bioshield requires that the DHS, in conjunction with the HHS, conduct a threat assessment to "assess current and emerging threats of chemical, biological radiological, and nuclear agents; and determine which of such agents present a material threat against the United States population sufficient to affect national security" and for which a countermeasure is needed. As implemented, this threat assessment must be conducted prior to any decision to purchase a needed countermeasure under the Project Bioshield.

It is my understanding that, to date, no such assessment has been conducted to determine the threat of cyanide to the American people. Aside from cyanide's historical use as a battlefield weapon in World War I, this country has already suffered from terrorist attacks and plots using cyanide: in the 1980s, with the tampering of Tylenol; in 2003, with the discovery of a cyanide bomb in the possession of a white

supremacist in Texas that held enough cyanide to fatally gas everyone in a 30,000 sq ft facility; and, in early 2004, with the discovery by U.S. troops in Baghdad of a 7-pound block of cyanide salt. Moreover, soon after our successful liberation of Afghanistan in 2002, our forces discovered Al Qaeda training videos using cyanide to poison dogs and other animals.

I note that in the legislative history of the Project Bioshield, a potential treatment for cyanide poisoning, hydroxocobalamin is specifically identified in the reports filed by the House Committees on Government Reform and Energy and Commerce. Thus, providers of this countermeasure are "on hold" pending completion of this threat assessment. Providing this information to industry will aid industrial base planning efforts and thereby promote the Project Bioshield Act's objective of fostering the development of a biodefense industry.

In addition to the specific recommendations above that should be taken into account during regulatory process and in order to carry forth the initiative's legislative intent, we have several policy suggestions that should be considered in implementing Project Bioshield: HHS should keep in mind that the government's use of multiple countermeasure suppliers and technologies would be in the overall interests of public health and homeland security. As evidenced by the recent influenza vaccine shortage, having a diverse "portfolio" of countermeasures in the strategic national stockpile will facilitate flexibility in responding to bioterrorism threats and attacks.

First and foremost, HHS should make clear that the statute does not require contractors to comply with burdensome government procurement requirements, including the requirement for certified cost and pricing data, in order to stimulate the maximum interest possible by commercial companies. Similarly, HHS should avoid the use of cost-type contracts or contract line items (thus, eliminating the need for a proposed contractor to adopt non-GAAP accounting practices) wherever possible.

HHS should structure Bioshield contracts to avoid a "staged" procurement approach such as that announced in the recent Anthrax therapeutic request for proposal, wherever possible. While we recognize the need for staged procurements under certain circumstances, using this method where HHS has conducted proper market research will avoid unnecessary delays and unpredictable results, thereby stimulating far greater private sector interest.

Maximizing the use of these authorities, as well as enactment of the additional streamlined authorities identified above, will go a long way to ensuring the greatest possible participation in Bioshield. Moreover, as we have already seen in how slow the contracting process has been to date with Bioshield, failure to act on these procurement reforms will cost the Nation something that no amount of money or any act of Congress can ever make up for time.

I very much appreciate the opportunity to offer testimony on this very important public health and anti-terrorism issue. Achieving the objectives of the Project Bioshield Act of 2004 and Senate Bill 3 are of the utmost importance to ensuring homeland and national security. Again, I applaud your efforts, and the efforts of President Bush and his Administration, and look forward to continuing our work with Congress and the Administration in this critical area.

I am happy to respond to any questions you may have.

PREPARED STATEMENT OF THE SARNOFF CORPORATION

Chairman Gregg, Ranking member Byrd, Sarnoff Corporation appreciates the opportunity to offer testimony on "BioShield and Bioterrorism." Sarnoff Corporation (www.sarnoff.com) produces innovations in information, biomedical, and electronic technology that generate successful new products and services for clients worldwide. Founded in 1942 as RCA Laboratories, Sarnoff has been serving both the public and private sectors to develop breakthroughs in integrated circuits, lasers, and imagers; drug discovery and development; digital TV, video for security, surveillance and entertainment; high-performance networking; and wireless communications. Our history includes the development of color TV, liquid-crystal display, and the disposable hearing aid, as well as a leadership role in creating the U.S. digital television standard. With the Rosettex Technologies and Ventures Group (a joint venture with SRI), Sarnoff has demonstrated a unique ability to bring a broad range of private sector organizations together to accelerate technology development in the interest of the national security. As discussed below, we believe that these skills are vital to the Nation's ability to meet the bioterror threat.

As a science and technology leader, Sarnoff recognizes the serious danger posed by bioterrorism and emerging infectious diseases to the United States. In addition to the many infectious agents already recognized as threats, new agents, like the

SARS coronavirus and the avian flu continue to emerge. Moreover, the bioterrorist threat includes the growing potential to use biotechnology to create new, genetically engineered pathogens against which existing countermeasures are ineffective.

To effectively secure our Nation against the threat of bioterrorism, in addition to developing countermeasures for all existing threats, it will be necessary to rapidly develop, manufacture, and distribute new countermeasures to treat illness and prevent further infections in the population for those agents we cannot predict. However, today it takes an average of 10 years to develop a countermeasure for a new agent. Clearly, this process must be accelerated if the entire spectrum of the biothreat, not just the set of currently recognized agents, is to be defeated.

Sarnoff believes that the countermeasure development process can be significantly shortened with a focused effort. For this reason, we are highly supportive of the inclusion of the concept of "research tools" in S. 3 and other legislative efforts seeking to improve the Nation's biodefense. Research tools are integral to the drug and vaccine development process, and thus an essential focus of all efforts to accelerate this process. The concept of research tools includes not only animal models and in vitro tests, but also technologies that reside outside the laboratory or in computers, such as bioinformatics and toxicological databases and drug and disease modeling systems. In addition, the use of new technology and methods in the clinical setting and during manufacturing will have crucial roles to play in accelerating development. While new animal models are essential for approval of needed countermeasures under FDA's current Animal Rule, ultimately research tools will help us move beyond the existing regulatory system by enabling much faster, less expensive, but highly reliable routes to new countermeasures. The FDA's 2004 report, Innovation or Stagnation? The Critical Path to New Medical Products lays out a vision of faster translational research and improved product development, and calls for better research tools for determining safety and efficacy and new manufacturing processes.

Determining what research tools are necessary to shorten the countermeasure development process is a significant challenge. Drug and vaccine development is extremely complicated, highly diverse, and multidisciplinary, involving hundreds of different types of technology and areas of scientific expertise. Along the pathway, roadblocks and time-consuming steps, often referred to as "bottlenecks," are multiple and interconnected. We believe a systems approach is required to address what is essentially a complex systems problem. Research tools must be integrated into end-to-end systems in order to move from the local acceleration of the development process that is current practice to substantial, overall reductions in the drug development cycle.

The development of research tools and research tool systems requires more than just scientific and technological advancements. It requires a well coordinated and tightly orchestrated national strategy designed to encourage and support creation of these systems. That coordinated national strategy is not yet in place.

Further, Sarnoff believes an unprecedented public-private partnership will be required not only to bring new research tools and research tool systems into use, but also to enable their application to rapid development of production of life-saving countermeasures in the event they are needed in a national public health emergency.

In summary, the Sarnoff Corporation thanks you, Mr. Chairman, and the Committee for the opportunity to submit this statement for the record of this important and very timely hearing. We look forward to working with you and your colleagues in ensuring that the threat bioterrorism and infectious disease pose to national security and the public health is adequately addressed, mitigated, and, ultimately, eliminated.

THREATS IN ORDER OF PRIORITY

Senator GREGG. Thank you and thank all members of the panel for what were very informative presentations. Hopefully there is somebody here from HHS and Homeland Security listening to it besides just those of us in Congress who try to get their attention. I think some excellent points were made.

Dr. Franz, you essentially seem to be attracted to the second approach here, which you outlined, which is to pick off the major threats and try to come up with ways to address those rather than a more global approach. You mentioned smallpox and anthrax as being obvious areas to start with and where we do appear to have

started and made progress. Dr. Read said, but what is next, and the market does not know what is next.

Is it possible, with your years of experience in the Government, to get an agreement as to what the threats are in order of priority for, say, the top 10 potential pathogens so people could predictably start to look at those, if they are in the scientific community, as places where they might want to put some resources to develop responses?

Dr. FRANZ. Senator, I believe as I mentioned, there are clearly outliers. The two that we all agree on are well above many of the others in my opinion, and that is based on the characteristics of the organisms. I really do not know anything about the likelihood of their being used, but we would have enormous vulnerabilities to those and likewise, as the last speaker mentioned, influenza. I think we would have enormous vulnerabilities there as well.

Senator GREGG. So should we go beyond those pathogens? Should we just do those three then and get ready for those?

Dr. FRANZ. I think if you start into plague and tularemia and Q fever and even botulinum—most of my lab work was done back at the bench at USAMRIID before I moved into the front office with bot. I do not put that up as high as these others, and it is because of the characteristics of the organisms, how difficult they are to grow, how easy they are to treat, how stable they are in the environment and so on.

So I think it becomes so hard and so expensive to produce specific countermeasures for those we do not consider outliers that I prefer a broad, general approach to public health for those, after we have dealt with the outliers. That should include good diagnostics, good disease surveillance, good epidemiology, and the same kinds of things, good education for our health care providers and for our citizens, the same kinds of things that help us in any emerging outbreak.

So I am a believer in very specific countermeasures for those that are really tough to deal with and then very broad preparedness for those which are easier to deal with and harder to pick as potential threats.

Senator GREGG. That sounds like a rational approach, and it is sort of the approach we are taking. Is it not?

Dr. FRANZ. I think it is, and I am happy with that. In that regard, I am actually involved at the S&T review for DHS programs for Secretary McQueary's program here today, and about 6 weeks ago, I was in Galveston to review the RCE meeting which is the Fauci $1.5 billion or $1.8 billion basic R&D program. Academe is heavily involved in both of these, and I have really been quite pleased with the fundamental research going on out there. We have some of our best scientists in the country stepping forward as the Nation needs them to contribute.

As the other speakers have said and as I learned in the military, the hard part is transitioning that good basic research into the arms or into the airwaves of our citizens to protect them, and that is where we need the most help I think.

INDEMNIFICATION

Senator GREGG. Well, the first part is good news, and the second part is Dr. Read's job since he is the investment guy here.

You listed a whole series of points, Dr. Read, as to how we could create a better climate for getting people to pursue these and move them to commercialization, if that is the right term. Probably not, but at least to being used.

Would you put indemnification at the top of that list?

Dr. READ. Maybe because it is a non-starter without. So there are many important things needed to be done to enhance BioShield in order for it to meet the test of drawing in our most capable innovators into this fight. So dealing with product liability and indemnification is clearly going to be necessary to have large, capable companies join the fray.

Senator GREGG. And next on the list would be what? The need to know what the targets are, targets of opportunity, so to say?

Dr. READ. Well, it is nice put next because it is clear and somehow we ought to be able to do it. I do not understand why the private sector should have to guess what the Government is thinking about these priorities. So I would put it second for clarity and because we ought to be able to check that box off.

I think one of the best ways it can be signaled is through the economic incentives that our public servants can send using the legislation and the funds available through BioShield and whatever improvements you are working on. The clear economic signals about a market, a reward at the end is by far the most compelling way to communicate those priorities, as opposed to a list. So if we knew the reward that had been created by the Government because it cared so much about, just for example, pick an agent on that list, tularemia or ebola or something, was twice the size of the financial incentive to succeed with a vaccine against another one, that would be about as clear a way to send those priorities as possible. And it would be incredibly useful not only if the reward were big enough and product liability were dealt with. I sincerely believe our largest and most capable companies would engage.

The truth is the market signals are used all the time to make portfolio decisions inside large companies and small ones. And if the large companies are there, the small ones will be there, the companies I invest in, because the small companies often make the key early-stage contributions that enable the larger companies to finish the job.

RISK OF LIABILITY

Senator GREGG. Which brings us to Mr. Clerici's point, which is that the big companies are not in there and the reason we have lost our vaccine industry in this country is the liability and the fact that the risk of liability so far exceeds the risk of return that there is no way to get people to put capital into this market.

Do you think we need to go beyond what we have in S. 3 or do we have enough in there on this liability? I mean, we know this whole liability fight is an uphill fight in the Senate, period.

Mr. CLERICI. Right. The approach that you take in S. 3, whereby a winner of a BioShield contract is automatically protected from li-

ability, so it is based on the same theories as the SAFETY Act, but without the same hurdles, I think would provide the necessary incentives for manufacturers to get into the biodefense market, large and small, because there at least would be some certainty that, assuming that you deliver, this liability protection is forthcoming automatically. I will put aside the political challenges of a system such as that which amounts to, more or less, tort reform rather than an indemnification scheme such as present with smallpox or under Public Law 85–804.

ADDITIONAL COMMITTEE QUESTIONS

For pandemic flu, I am not sure it is going to be enough because the providers of that vaccine know at the end of the day their vaccine is going into the arms of 300 million people. Even under the legislation proposed in S. 3, you are still going to be in Federal court defending those lawsuits throughout the country. So the predictability of what a Federal judge may do with the legislation and the fact that the plaintiffs could certainly file litigation in every jurisdiction throughout the land would be problematic to those companies. And the companies that are primarily going to supply the pandemic flu vaccine are the largest of the vaccine manufacturers and therefore have the most shareholders and the most concerns, being a large public company.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing:]

QUESTIONS SUBMITTED TO DR. PENROSE C. ALBRIGHT

QUESTIONS SUBMITTED BY SENATOR JUDD GREGG

Question. Which Federal agency determines the bioterrorism threat and the Federal response to that threat?

Answer. Homeland Security Presidential Directive 10 (HSPD–10), Biodefense for the 21st Century, identifies the Department of Homeland Security as the lead Federal agency for "conducting threat periodic assessments of the evolving biological weapons threat" and for "developing comprehensive plans that provide for seamless, coordinated Federal, State, local, and international responses to a biological attack."

Question. Under what authority is the Department of Homeland Security (DHS) involved in responding to bioterrorist threats?

Answer. DHS authority to respond to bioterrorist threats traces originally through Section 502 of the Homeland Security Act of 2002 which states that "The Secretary, acting through the Under Secretary for Emergency Preparedness and Response, shall include . . . (3) providing the Federal Government's response to terrorist attacks and major disasters" and has been reaffirmed specifically for biological attacks in the HSPD–10 as cited previously. This role is one of providing overall coordination with the individual Sector Specific Agencies executing their legislated responsibilities, e.g. the Department of Health and Human Services is responsible for public health and the Environmental Protection Agency for decontamination.

Question. How is a biological threat addressed once the threat has been determined and what avenue does DHS use to respond to that threat?

Answer. Once a biological threat has been determined, it becomes a potential or actual Incident of National Significance and DHS becomes responsible for the overall coordination of the response. This is done under the framework of the National Incident Management System (NIMS) using the National Response Plan (NRP). The NRP provides the coordinating structure and mechanisms for national level policy and operational Federal support to state, local and tribal incident managers. The Homeland Security Operations Center (HSOC) serves as the primary national-level multi-agency situational awareness and coordination center. Other key coordinating mechanisms include: the Interagency Incident Management Group (IIMG), a senior level interagency group who provide strategic advice to the Secretary of DHS; a

Joint Field Office (JFO), a temporary Federal facility established locally to provide a central point for Federal, State, local and tribal representatives responsible for incident support and coordination; and a Principal Federal Officer (PFO), designated by the Secretary of DHS to work in conjunction with other Federal officials to coordinate overall Federal incident management efforts. The Federal response to actual or potential Incidents of National Significance is typically provided through the full or partial activation of the Emergency Support Functions (ESF). The NRP applies a functional approach that groups the capabilities of Federal departments and agencies, as well as the American Red Cross, into ESFs to provide the planning, support, resources, program implementation, and emergency services that are most likely to be needed during an Incident of National Significance. Each ESF is composed of primary and support agencies, based on their authorities, resources, and capabilities.

The NRP also includes a Biological Incident Annex, which outlines the actions, roles, and responsibilities associated with response to a disease outbreak of known or unknown origin requiring Federal assistance. The annex outlines biological incident response actions, including threat assessment notification procedures, laboratory testing, joint investigative/response procedures, and activities related to recovery. Because of its authorities, capabilities, and resources, the Department of Health and Human Services is the lead agency for the Biological Incident Annex.

Question. What role does DHS' Science and Technology (S&T) Directorate play regarding research into bioterrorist threats?

Answer. The S&T Directorate plays a major role in research into bioterrorist threats. The S&T Directorate is the national lead for the periodic assessments required by HSPD–10 under its Threat Awareness Pillar. These assessments include formal Risk Assessments every 2 years, with the first due in January of 2006, and Net Assessments every 4 years, with the first due in 2008. Under the BioShield Act of 2004, DHS is also responsible for making the Material Threat Determinations (MTDs) that inform the Department of Health and Human Services as to which agents are of especial concern as to warrant pursuit of medical countermeasures utilizing BioShield funding. To support and inform its assessment roles, the S&T Directorate also conducts research to improve the Nation's understanding of critical agent properties that might have a significant impact on its defense and response, e.g. the infectivity of agents at low doses or how long an agent survives in air, food or water.

SCIENCE & TECHNOLOGY DIRECTORATE AND INTEGRATED BIOSURVEILLANCE

Question. Can you provide the Committee an update on the status of Integrated Biosurveillance?

Answer. The Information Analysis and Infrastructure Protection Directorate (IAIP) of DHS is implementing the National Biosurveillance Integration System (NBIS) to integrate biosurveillance information with the objective of identifying and characterizing a biological attack on the Nation. The NBIS implementation is closely aligned with the NBIS design effort that was led by the S&T Directorate in 2004, with the full participation of the interagency partners. Currently, IAIP is in the procurement process for the NBIS system.

DEPARTMENT OF HOMELAND SECURITY AND BIOSHIELD

Question. How does the National Biodefense Analysis and Countermeasures Center, or NBACC, fit into the Department's role in defending against a bioterrorist threat?

Answer. The National Biodefense Analysis and Countermeasures Center (NBACC) is one of the Department's and the Nation's key tools in defending against bioterrorism. NBACC consists of two centers: the BioThreat Characterization Center (BTCC) and the National BioForensics Analysis Center (NBFAC). The BTCC is responsible for the threat characterization activities described previously, i.e. for conducting the periodic Risk Assessments required under HSPD–10 and for the scientific research to inform these threat assessments and support intelligence activities. The NBFAC, as designated under HSPD–10, is the lead national facility for conducting technical analysis of forensic materials to support attribution by the appropriate Departments and agencies. As such, the NBFAC is operated in close coordination with the Department of Justice's Federal Bureau of Investigation and with portions of the Intelligence Community.

Question. Since its inception, the NBACC has received $130 million in Federal appropriations from various sources, beginning with work conducted by the Department of Defense (DOD). Given the current research conducted by the Army at Fort

Detrick, is there any duplication of effort between what the Army does and what is proposed for the NBACC facility?

Answer. The Department of Homeland Security (DHS) National Biodefense Analysis and Countermeasures Center (NBACC) and the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) fulfill complementary but distinct missions at the Fort Detrick National Interagency Biodefense Campus (NIBC), where Congress has identified the need for Federal agencies to work collaboratively to address the threat of bioterrorism.

NBACC conducts research to protect the American public by enhancing our scientific understanding of biological threats. This complements, not duplicates, USAMRIID biodefense research and development and test and evaluation to provide medical protections such as vaccines, drugs, diagnostics, and information for military service members. Unlike USAMRIID, NBACC does not perform research to develop medical countermeasures.

NBACC threat characterization research provides a scientific basis to understand current and future biological threats, to assess vulnerabilities, and to determine potential impacts. Moreover, NBACC threat characterization supports DHS material threat assessment responsibilities under the BioShield Act.

NBACC bioforensic research provides a national capability to conduct forensic analysis of bio-crimes and terrorism to attain a "biological fingerprint" to identify perpetrators and determine the origin and method of a terrorist attack. HSPD–10 designates NBACC's National Bioforensic Analysis Center to be the lead Federal facility to conduct and facilitate forensic analysis of biological terrorism.

Question. How does the Department address its responsibilities for dealing with a biological threat to our agricultural infrastructure?

Answer. As specified in HSPD–7 (Critical Infrastructure Identification, Prioritization and Protection), the DHS Information Analysis and Infrastructure Protection Directorate (IAIP) has the lead DHS role for vulnerability assessments and protection of the Nation's critical infrastructure, and has led the inter-agency effort to develop a National Infrastructure Protection Plan (NIPP; sector-specific plans for agriculture and food are now in preparation). IAIP also has the DHS lead role for outreach to the private sector, including the development of a Food and Agriculture Sector Coordinating Council (F&ASCC) to facilitate information sharing between government and the private sector, and a Government Coordinating Council (GCC) to facilitate coordination across government and between government and the sectors. A "food and agriculture portal" has been created for the Homeland Security Information Network (HSIN) to provide a platform for the secure sharing of information (e.g., alerts, warnings, incident reporting, event tracking, etc.), and a Protected Critical Infrastructure Information (PCII) classification for the protection and special handling of proprietary industry information (e.g., vulnerabilities, threats).

And, as specified in HSPD–9 (Defense of United States Agriculture and Food), the S&T Directorate has responsibility for the overall inter-agency coordination to "accelerate and expand development of current and new countermeasures against the intentional introduction or natural occurrence of catastrophic animal, plant, and zoonotic diseases." Since June of 2003, the S&T Directorate has been responsible for the operation and management of Plum Island Animal Disease Center (PIADC) and has developed a joint research and diagnostic strategy with USDA (Animal Research Service and the Animal and Plant Health Inspection Service) for foreign animal diseases (FAD). Together with USDA and HHS, we have also begun the conceptual design of the next generation National Bio and Agro-defense Facility (NBAF) needed to replace the aging PIADC. Other major S&T Directorate agricultural thrusts include: systems studies, coupled disease and economic models, and table top exercises to better understand outbreak control options and inform policy and decision makers; demonstration of high throughput detection to better control and respond to outbreaks of foreign animal disease; detection systems for monitoring critical food nodes in the processing and distribution of selected food products; and two University Centers—one on foreign animal and zoonotic diseases and the other on food protection—to provide longer term research and train the next generation of agro-defense researchers and practitioners.

As specified in HSPD–5 (Management of Domestic Incidents), DHS has developed a framework for overall national coordination. This framework is established in the National Response Plan (NRP) and National Incident Management System (NIMS). The NRP includes Emergency Support Functions (ESF) to organize and provide Federal resources during responses (e.g., ESF–8, "Health & Medical Services", DHHS lead; and ESF–11, "Agriculture and Natural Resources", USDA lead) and Support Annexes to insure efficient and effective incident management (e.g., "Science and Technology", DHS Science and Technology Directorate (S&T) lead).

Question. Who determines which vaccines are placed in the National Stockpile and what's the Department's role in that decision, given its responsibility for determining the bioterrorism threat?

Answer. The process to determine which vaccines are placed in the National Stockpile is determined by the Centers for Disease Control and Prevention (CDC) within the Department of Health and Human Services (HHS). Recommendations for advance development of chemical, biological, radiological, and nuclear (CBRN) countermeasures utilize the Weapons of Mass Destruction Medical Countermeasures (WMD MCM) Subcommittee. This is an interdepartmental subcommittee initially chartered by the National Science and Technology Council (NSTC) and co-chaired by senior government officials from the Department of Homeland Security (DHS), the Department of Health and Human Services (HHS) and the Department of Defense (DOD). The material threat assessments (MTA) developed by the DHS based on a plausible attack scenario informs the sizing of the requirement. The HHS then evaluates the availability of current countermeasures and the possibility of development of new countermeasures. The WMD MC subcommittee deliberates on the nature of the medical consequence and the availability of appropriate countermeasures to develop a recommendation for the acquisition of a specific countermeasure. The HHS can issue a Request for Information (RFI) to determine the market availability and to alert industry to the U.S. Government interests. A Request for Proposals (RFP) announcing the specific requirements will then follow, once a U.S. Government requirement for a particular new medical countermeasure has been established by the WMD MC subcommittee, and approved by the Office of Management and Budget (OMB). The HHS implements the acquisition process.

Question. Explain the steps in developing and putting into the stockpile new medical countermeasures. Who has the lead at each step? I understand the role of the National Institutes of Health (NIH) in basic research, but how is that science translated into product?

Answer. The science and research to develop a new medical countermeasure will most likely have been supported by the National Institutes of Health (NIH) or the U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID); however many industrial initiatives are launched independently to develop a new product. In order to translate a basic science advancement into a viable product, certain applied research and advanced development is required. This process will focus on establishing a "formulation" for the product and a scalable manufacturing process utilizing a Good Manufacturing Processes (GMP) validated process conducted under appropriate Quality Assurance and Quality Control activities. In addition the appropriate animal studies and human safety studies need to be conducted in accordance with FDA regulations to assure that the results can be applied to regulatory decisions. The ability to manufacture a consistent and stable product is also evaluated. Please consult HHS for a more complete description.

Question. Does BioShield sufficiently incentivize industry to develop countermeasures to the bioterrorism threat?

Answer. This question is perhaps best answered by industry. However, Project BioShield is a good first step and has sent a message to industry that the U.S. Government is committed to obtaining appropriate countermeasures for the Strategic National Stockpile (SNS). The establishment of a 10 year special reserve fund of $5.6 billion provides confidence to industry that acquisition funds are available in the long-term. Ten months after the enactment of the Project BioShield Act, the U.S. Government awarded three contracts totaling over $1 billion for SNS acquisitions. Negotiations are in progress for two other contracts. In addition, two RFIs and one draft RFP have been recently published.

Question. What is the appropriate Federal role regarding research and development of countermeasures for the National Stockpile?

Answer. The role of the U.S. Government regarding research and development for countermeasures has traditionally been through the support of basic research. Both NIH and DOD (USAMRIID, USAMRICD, and AFRRI) have excellent records in this regard. The U.S. Government can further target and facilitate research and development (R&D) efforts by setting clear requirements and specifications for medical countermeasures; facilitating partnerships as needed between government and industry or between differing industries; and providing critical resources such as facilities (e.g. biocontainment labs), animals (for testing), reagents and assays.

Question. How does the Department address the development of countermeasures as it relates to industry disparities regarding large and small companies and their available capital for research and development?

Answer. Human medical countermeasures development is done through HHS and DOD and not through the Department of Homeland Security, so we will defer to them on the medical portions of this answer. For non-medical countermeasures, the

S&T Directorate does not require nor expect cost sharing in our R&D programs. A company's available capital to co-fund R&D is not an issue. Our competitive solicitations for all kinds of countermeasures research and development have offered multiple opportunities for both large and small businesses. Competitive solicitation results show that for research and development in highly technical fields, small companies can successfully compete outright, and this is especially true when they partner with larger or other small businesses.

Question. From your perspective, how has BioShield helped DHS respond to the bioterror threat? Is it working as intended, and what would BioShield II do for DHS and S&T specifically?

Answer. BioShield is helping DHS respond to bioterror threats by stimulating the development of needed medical countermeasures, by providing for emergency use authorization of these and other countermeasures if needed, and by streamlining the review process for research related to future generations of medical countermeasures for these threats. Procurements are now in progress for botulinum antitoxin, the current generation anthrax vaccine (AVA), the next generation anthrax vaccine (rPA) and for a pediatric formulation of potassium iodide—a therapeutic for certain kinds of radiation exposure. A Request for Information has recently been issued for a third generation smallpox vaccine (MVA) which would further minimize any side effects. Also, earlier this month, the National Institute of Allergies and Infectious Diseases (NIAID) made its first series of research awards using its new BioShield authorities.

Question. Please provide a list of administrative, regulatory and legislative proposals needed to invigorate scientific research relevant to the development of needed countermeasures and products to counter natural pandemics and epidemics.

Answer. The Nation has a strong program in basic scientific research related to the development of medical countermeasures. There are broad activities in understanding the genomics and proteomics of microorganisms. In addition many research programs are focused on the understanding and control of the immune system. Advanced research and development however falters after the proof of principle stage when applied product development activities are required. Additional attention is needed in areas critical to mid-stage development of medical countermeasures such as animal studies, clinical studies, regulatory issues and the need to establish and validate a GMP (Good Manufacturing Processes) production process.

Question. I understand that you are the lead DHS representative for an interagency working group on bioterrorism and bioterrorism countermeasures. I also understand that the U.S. Department of Health and Human Services (HHS) and DOD participate in this working group. Can you tell me who else is involved in the working group, how often you meet, and what the basic function of the group is?

Answer. Recommendations for advance development of CBRN countermeasures utilize the Weapons of Mass Destruction Medical Countermeasures (WMD MCM) Subcommittee. This is an interdepartmental subcommittee initially chartered by the National Science and Technology Council (NSTC) and co-chaired by senior government officials from the Department of Homeland Security (DHS), the Department of Health and Human Services (HHS) and the Department of Defense (DOD). The material threat assessments (MTA) developed by the DHS based on a plausible attack scenario informs the sizing of the requirement. The HHS then evaluates the availability of current countermeasures and the possibility of development of new countermeasures. The WMD MC subcommittee deliberates on the nature of the medical consequence and the availability of appropriate countermeasures to develop a recommendation for the acquisition of a specific countermeasure.

DEPARTMENT OF HOMELAND SECURITY, BIOWATCH, AND DETECTION OF EVENTS

Question. How does DHS respond to recent criticism in the press that BioWatch is not effective?

Answer. BioWatch has been deployed to over 30 cities and provides these cities with protection against biological threat agents. At the request of the stakeholders, additional assets currently are being installed to provide increased coverage to include high trafficked facilities and other venues that attract large numbers of the population. DHS believes that BioWatch is an effective system which will be further improved by enhanced coverage while maintaining the no system false positives to date after conducting over two million assays.

Question. What kind of measures are in place to assist the Department in its coordination role regarding BioWatch?

Answer. Formal BioWatch coordination is done officially through a Memorandum of Understanding with the DHS, HHS/CDC, and EPA. Roles and responsibilities are

articulated and budgetary aspects addressed. Additionally, the BioWatch Office works closely with CDC and EPA regarding day to day operations, enhancement of the current program, and future capabilities, thus ensuring success through close ties with the partners. Supported by a HSC Biodefense Memorandum of Understanding, the S&T Directorate also is actively engaged with USPS, DOD, HHS, and DoJ to discuss technology R&D programs and interoperability, concept of operations to include notification, and the development of a national architecture.

DEPARTMENT OF HOMELAND SECURITY'S ROLE IN DETECTION EQUIPMENT

Question. Given the overarching responsibility the Department has regarding biodefense, what is the Science and Technology Directorate's role in the development and evaluation of biological threat detection equipment?

Answer. The S&T Directorate's role in the development and evaluation of biological threat detection equipment is to enhance current systems capabilities while developing the next generation of detection systems to provide early detection of attacks on outdoor and indoor areas and on our agricultural and food infrastructures. Currently, S&T Directorate efforts include: detection systems to enable the next generation of BioWatch, our urban monitoring program; the development of rapid (in minutes) identifiers for protection of high valued facilities and special events, and the development of detection systems for food distribution systems. Additionally, the S&T Directorate has a robust bio-assay development program which both supports our current biomonitoring systems such as BioWatch and is also integrated with the Directorate's detection technology development programs. The S&T Directorate, working through the Association of Analytical Chemists (AOAC), has also taken the lead in testing and evaluating hand-held assays for screening of so called "white powder" events.

The S&T Directorate participates routinely on interagency working groups through the Homeland Security Council (HSC) and Office of Science Technology Policy (OSTP) to help establish and coordinate biodefense detection strategies and requirements. A major recent accomplishment in this area is the signing of a Memorandum of Understanding for Coordinated Monitoring of Biological Threat Agents Amongst the Department of Homeland Security, the Department of Health and Human Services, the Department of Defense, the Department of Justice and the United States Postal System. The S&T Directorate also interacts regularly with the detection development, test and evaluation programs in the DOD and the EPA (e.g. the Environmental Testing and Verification Program), including mutual participation in each others program reviews. S&T Directorate staff members routinely monitors literature, attend technology conferences, and host members from industries, academia, and non-profit organizations which present their current efforts and findings in technology development.

Question. How does the Directorate foster the growth in biothreat detection equipment, and how do you respond to a rapidly changing industry?

Answer. The S&T Directorate fosters the growth in bio-threat detection equipment through two key steps (1) a clear formulation and communication of our needs and requirements; and (2) an active, multi-pronged, outreach to the broad R&D community for the best way to meet these requirements in a timely fashion. Through systems studies and scientific and interagency committees, we have focused on three classes of detection systems that are critical to an integrated national biodefense: advanced detection for monitoring urban areas; rapid (minutes) identification for protecting key facilities and special events; and detection systems for protecting our agricultural and food infrastructures. Detailed performance and cost requirements have been formulated to inform industry, academia and the national and Federal laboratories of our needs and have been published on the S&T Directorate's Homeland Security Advance Projects Research Agency (HSARPA) website. The S&T Directorate has had broad solicitations in each of these areas, typically involving an open, national level workshop conveying the needs and asking for inputs and refinements from the participants, a formal Request for Information (RFI), and then a formal proposal solicitation. Hundreds of proposals have been received and evaluated, with some fifteen proposals already funded and others in the works. The focus is on applied research with a goal of fielding technology as rapidly as possible, typically within 3 to 5 years. A phased development approach is used. The technology developers are evaluated and down selected by rigorous testing during each phase (Preliminary Design Review, Critical Design Review, etc.). Each technology does receive feedback during the testing at each phase with an opportunity for adjustments and re-evaluation. However, candidate technologies will be terminated if they fail to show reasonable progress. The S&T Directorate will also consider testing technologies funded through other programs (from other organiza-

tions) against the goals set forth by the S&T Directorate. In parallel, the S&T Directorate participates in a range of technical conferences and discussions with developers of detection systems to stay abreast of any developments that might change how it thinks about the realm of the possible' in both near- and longer-term biodetection system. The S&T Directorate believes the strategy outlined above provides both the guidance and the flexibility to foster growth and responsiveness in a rapidly changing industry.

Question. What role do the national labs play in this arena?

Answer. The national laboratories have played a key role in BioWatch sensor development and deployment and provide expertise on siting of detection systems. They continue to be a vital part of the S&T Directorate's strategy to develop and pilot advanced biothreat detection systems, with research and development activities in the following areas:

—Development of specific instrumentation (Biobriefcase, Enhanced BioAerosol Detector): Lawrence Livermore National Laboratory (LLNL) and Sandia National Laboratory (SNL).

—Development of new nucleic acid- and protein-based assays of recognized biothreat agents to be used in biodetection instruments: LLNL, Los Alamos National Laboratory (LANL), Pacific Northwest National Laboratory (PNNL), and SNL.

—Identification of next-generation signatures that reflect either (a) the host-pathogen interaction or (b) virulence characteristics or antibiotic resistance of recognized or emerging biothreat agents and using these signatures to develop new assays for biothreat detection: LLNL and PNNL.

—Provision of informatics support to enable the discovery of new targets for assays and to develop new reporting tools for detection instruments: LLNL, LANL, Lawrence Berkeley National Laboratory (LBNL), PNNL, and Oak Ridge National Laboratory.

Question. Without getting into classified information, please tell us how we are doing in the deployment of surveillance and detection equipment.

Answer. In January and February 2003, BioWatch was deployed to approximately 30 U.S. cities. At that time, a limited number of collectors were strategically placed in each city to provide for maximum population protection. At the request of the BioWatch cities, a Generation (Gen) 2 BioWatch was developed to provide increased temporal and spatial coverage and was piloted in New York City in fiscal year 2004 and early fiscal year 2005. Gen 2 increases the number of collectors two to fourfold, including coverage of key priorities identified by the cities, such as transportation hubs and other indoor venues that are highly trafficked. Gen 2 is in the process of being deployed to the top threat cities in fiscal year 2005 and fiscal year 2006. Additional samplers will be placed in each BioWatch city to be used at special events and/or at the cities' discretion. New technology is now under development that will enable a "Gen 3" BioWatch which reduces the sampling and analysis time to four hours on site and will be wirelessly networked to a local public health interface for further confirmation and so that positive samples can be retrieved for further analysis. This technology will provide for the high sensitivity and extremely low false positive rate consistent with the current system.

We are also developing other detection systems. High throughput diagnostics for agricultural testing will be piloted in fiscal year 2006 and food sensors for specific applications will be developed by fiscal year 2007. R&D is also on-going on detect-to-warn' sensors that can detect biological agents in a less than five minutes and hence be used to provide warning of releases in high value building, facilities, and special events.

Question. Have you done any evaluation or testing of surveillance and detection equipment once it's been deployed and is in use?

Answer. Yes, there is active evaluation and testing of the BioWatch system. The BioWatch Exercise and Evaluation Program (BWEEP) is an annual proficiency test for BioWatch laboratory and field operations and is designed to insure protocols and procedures continue to meet or exceed prescribed standards. If there are no deficiencies, they will not be revisited until the next annual cycle. If there are minor deficiencies, on-the-spot corrections or additional training will be administered and they will be re-inspected in approximately 6 months. If there are major deficiencies and/or safety violations, immediate remedial actions will be taken.

Question. What collaborative process does the Department use to gain the input from industry, researchers, and responders in the development of new technology? Does the process include peer review?

Answer. The Science and Technology Directorate uses an open and competitive solicitation process for research and development with the private sector.

Before the official solicitation is issued, the S&T Directorate may publish a draft Statement of Work for public comment, giving industry the opportunity to provide advice and recommendations. In appropriate cases, full scale technical workshops are held to assess the state-of-the-art, inform all potential bidders of current developments in the field, and sharpen the technical focus of the solicitation. In most cases, after each solicitation is published, a public Bidders' Conference is held to explain the solicitation in detail and answer questions that may have arisen in the minds of potential bidders. Each solicitation has an open Frequently Asked Questions (FAQ) section on the website where individual bidders' questions are answered and published for the benefit of all. In a typical solicitation procedure, the S&T Directorate uses the first bidder submission—the white paper—as a vehicle for discussion with private sector bidders. In addition, industry representatives are free to request direct interviews with S&T Directorate Program Managers to describe or discuss their concepts, ideas, and ongoing developments for new technologies.

The criteria by which white papers and proposals are evaluated by DHS technical experts are listed fully in the public solicitation so that bidders understand how their submissions will be judged. The S&T Directorate uses a technical merit review instead of peer review. Technical solutions to DHS needs and requirements often involve complex engineering, proprietary information, and other information of economic value to competitors. To perform technical review, the S&T Directorate organizes a panel of Federal Government experts, including S&T Directorate staff, other DHS technical and operational staff, and experts from other Federal agencies. The evaluation panel may be supplemented by outside advisors if there is a need for specialized expertise the government evaluators do not have. These outside advisors must agree that neither they nor their home institutions may bid against that particular solicitation. The S&T Directorate has found that providing review by government personnel, rather than a panel of peers, allows bidders to be more open about proprietary information supporting their proposed project.

Additionally, DHS and national laboratories are consulted frequently by the S&T Directorate to formulate the strategic direction of research, development, technology and evaluation (RDT&E) programs.

The science and technology needs of emergency responders are represented in the S&T Directorate by the Portfolio Managers. Other methods for collecting salient inputs include the annual Science and Technology Requirements Council, an annual joint conference with the Department of Justice, an annual conference to forecast S&T Directorate opportunities and major program direction to the industrial community, an intense 6 week effort each year involving the identification of responders' needs for rapid prototypes, and face-to-face contact with customers while working on current R&D projects.

Question. What types of detection equipment are most difficult to develop, and how is the industry responding to the demands of the requirements? For example, the drug/vaccine industry indicates that decades of research are required before a drug/vaccine becomes available in the market. Is that same time and financial investment required by other industries?

Answer. In general, any development program that deals directly with human health can take years of research, development, testing and evaluation prior to becoming available to the market because of extensive safety regulations. Instrumentation, including detectors for biological, chemical, and explosive threats, also has a difficult development schedule. Initial systems can be developed and deployed within the next few years, but it may take upwards of a decade to develop and deploy cost effective instruments with all the desired capabilities. The main reason is the requirement to achieve a high probability of detection and a extremely low probability of false alarms in instruments that are of sufficiently low cost that they can be widely deployed and used for continuous monitoring. This will require development of completely novel technologies or complex engineering projects.

SCIENCE & TECHNOLOGY DIRECTORATE AND STANDARDS

Question. Given that Science and Technology (S&T) Directorate's 2004 guidelines and standards for biological countermeasures have been in place for a year, please give us an assessment of the effectiveness and relevance to the standards issued by the S&T Directorate regarding biothreat agents? How has industry responded to them?

Answer. The S&T Directorate has a role and responsibility to ensure the effectiveness of biological countermeasures tools developed for and used by the homeland security community. By setting consistent and verifiable measures of effectiveness for basic functionality, minimum performance, interoperability, efficiency, sustainability, and appropriateness and adequacy for the task, standards improve the qual-

ity of homeland security systems and technologies. The S&T Directorate's Standards Program strives to enable the homeland security community to make informed equipment purchases by establishing minimum performance standards which can be linked to Federal grants programs so that equipment purchases comply with these minimum performance standards.

In 2004, the primary focus for Standards for Biological countermeasures revolved around developing minimum performance criteria for biological screening devices (specifically lateral flow immunoassays) used by first responders. In fiscal year 2004 and early fiscal year 2005, an interagency task force was formed to address the effectiveness and use of lateral flow immunoassays for the detection of Bacillus anthracis (anthrax) by emergency responders. The task force agreed upon and published accepted performance criteria associated with the hand held assays (HHAs). The HHAs were tested and evaluated against the accepted criteria and those results were also published. An effort was also initiated with the Center for Domestic Preparedness to develop a standard Bio-Protocol for first responders to use to guide their response to a suspicious powder incident.

The relevance and effectiveness of this important effort to develop and implement standards for biological field screening devices are clear. In the past these devices were procured in great numbers and often used incorrectly in the field by first responders to assess the biological threat associated with suspicious powders. Numerous false alarms were raised based on the results of these devices. Before these devices can be used in the field, first responders must understand their limitations, have a clear concept of how they are to be used, and be trained to use them properly. The S&T Directorate's effort to develop standards for the detection of anthrax using HHAs has given the homeland security community access to reliable information on how these devices perform and which devices met the performance standards. These standards are just a first step in ensuring confidence in the Nation's response to biological threats. There are numerous other types of biological countermeasures technologies to be evaluated against the range of biological agents. In addition, standard sampling protocols and standardized training must be developed and implemented.

Industry was heavily involved from the onset with the process of developing these standards. Manufacturers voluntarily attended the interagency task force meetings, provided technical feedback on the study design and testing protocols, and provided instruments for testing. The entire standards development process relied upon working in an open atmosphere and gaining consensus of the majority of the stakeholders. Results of the testing were supplied to the manufacturers in a clear and timely manner. Unfortunately not all of the devices met the published acceptance criteria and hence some manufacturers were disappointed with the outcome. However, most manufacturers have indicated a desire to improve their devices and enter into a second round of testing.

Question. How does S&T respond to the Department's Office of State and Local Government Coordination finding that its existing standards are inadequate?

Answer. The S&T Directorate acknowledges that the existing biological countermeasures standards only address the performance of one type of detection equipment to one type of biological agent. The S&T Directorate's Standards Program is building a long-term plan and process for the development of standards to ensure the effectiveness and performance of all critical biological countermeasures technologies for a number of biological agents. However, the standards development process relies on consensus building, an activity that is often time-consuming and costly. Therefore, standards development activities have focused to date on urgent, high priority areas. In order to validate the entire spectrum of biological countermeasures products and technologies, requirements for each of the technologies must be defined and consensus between the agencies on those requirements must be obtained. Additionally, standards need to be fully developed that are tested and evaluated for the various biological technologies, methods and processes. Also needed is the development of integrated policies and procedures based on conformance to the standards, and institute standardized training. All of these tasks are necessary and important and shall be incorporated in a long-term plan, but their accomplishment requires the necessary resources and cooperation of all of the key stakeholders. In addition, the Standards Program must assess and balance the need for standards in all homeland security areas based on the available resources. In the near future, (fiscal year 2005 and fiscal year 2006) the standards portfolio will address the need for standards for biological sampling activities and additional biological screening devices.

Question. Have any revisions or refinements been made to those standards?

Answer. The standards development process consists of a number of well-defined steps including periodic review and revision of standards when necessary. Revisions

or refinements have not currently been made to the published acceptance criteria for the performance of hand held immunoassays for the detection of anthrax. DHS intends to initiate a second round of testing of new and improved devices and will hold a meeting of the interagency task force to determine whether revisions are needed and incorporate lessons learned before the new round of testing is initiated. As always, voluntary consensus standards development is an open process, and interested stakeholders will have a means of providing comments and feedback on any necessary revisions or refinements.

Question. What process is used to update the biothreat standards?

Answer. Because DHS is not a regulatory agency, the process of updating standards will follow the voluntary standards development organization's guidelines. In the case of the hand held immunoassays, the Association of Analytical Chemists International (AOACI) was the standards development organization. Hence, the AOAC process to update the standards will be followed.

Question. Have end-users and industry found the biothreat standards useful in the development and use of new equipment? Can you give us an example?

Answer. End-users are now able to obtain reliable information on the performance of various manufacturers' hand held immunoassays before procurement. That information enables end-users to make knowledgeable decisions on whether to use these devices and if so which ones are most reliable. In addition, many of the manufacturers have indicated that they have already made adjustments to their technologies and are eager to submit the new and improved technologies for a second round of testing.

SAFETY ACT

Question. How much of the SAFETY Act has been implemented by the Department? Is it being implemented by industry, issue, or on an ad hoc basis?

Answer. The Department has placed significant emphasis on the full implementation of the Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act) and has accomplished much in an extremely short time period. In less than 15 months, the Department has established an Office of SAFETY Act Implementation (OSAI), which is responsible for administration of the program. The Department has developed, published, and implemented a proposed rule (July 11, 2003) and an interim rule (October 16, 2003) governing the implementation of the SAFETY Act. In addition, the Department is in the process of developing revisions to the current implementing regulations to address public comments and operational experience.

More than 450 experienced technical and economic reviewers have been vetted and are available to evaluate SAFETY Act applications in accordance with the statutory criteria. OSAI has designed a reviewer training program specific to SAFETY Act requirements that each reviewer is required to attend.

The Department initially developed a SAFETY Act application kit for use by interested parties and has since revised the kit. The revised application kit reflects substantial feedback from applicants and industry as well as our operational experience, and we expect it to provide applicants with better guidance and tools for a successful application. On December 13, 2004, a Paperwork Reduction Act notice for the revised version of the new kit was published in the Federal Register. Further, a web-based, interactive application process has been instituted that allows sellers to submit applications electronically, obtain automatic feedback on the status of an application, submit questions to a help desk to obtain assistance with navigating the application process, and provide access to resource documents and frequently asked questions.

Significant elements of the Department's SAFETY Act implementation include:

—*Website.*—The SAFETY Act website (www.safetyact.gov) contains the electronic application kit, reference materials, Frequently Asked Questions (FAQs), and specific instructions for applications submitted in connection with a procurement.

—*Help Desk.*—OSAI established a help desk that can be accessed by way of online forms, an e-mail address (helpdesk@safetyact.gov), or a toll free phone (1–866–788–9318). The Department has received much praise for the help desk. Applicants not only receive timely responses, but they can actually speak with a staff member.

—*Outreach.*—Throughout the past year, OSAI has made presentations at numerous SAFETY Act-relevant conferences, held meetings with applicants, and established internal procedures to ensure that each applicant has the opportunity to discuss an application with relevant staff early in the review process.

—*Pre-Applications.*—OSAI implemented a pre-application process designed to provide applicants with a quick assessment of the likelihood of its technology being

approved for Designation or Certification if a full application is filed. These pre-applications are processed within the 21 days advertised and, in addition to a written assessment, each applicant is given the opportunity for a personal debriefing on its pre-application. Early processing delays have been eliminated—essentially all of the approximately 120 pre-applications filed since March 1, 2004, have been completed on time.

—*Application Kit.*—The initial application kit was designed with the expectation that changes would be required as operational experience was obtained. During the past year, OSAI has sought input from applicants, industry, and government on areas appropriate for revision. Utilizing this input and its own operational experience, OSAI prepared a revised Application kit in concert with the proposed revision to the interim rule. The Paperwork Reduction Act notice for the final version of the new kit was published in the Federal Register on December 13, 2004, and the Department anticipates early adoption of the new kit.

The SAFETY Act requires the Department to evaluate technologies on an application by application basis; however, the Department has undertaken a significant effort to coordinate the SAFETY Act application process with major anti-terrorism procurements where multiple Sellers will be providing the same technology to ease the burden on applicants and speed the evaluation process.

To date, the Department has received more than 200 pre-applications and 94 full applications. As of June 18, 2004, twenty Designations and Certifications have been granted and five applicants have received Designation only.

Question. How is the SAFETY Act being applied to Project BioShield products?

Answer. The Department is not aware of any application submitted in connection with the BioShield program. Any provider of an anti-terrorism technology may apply for the protections afforded by the SAFETY Act and it is reasonable to anticipate that participants in the BioShield program will apply for SAFETY Act protections as their technologies mature.

Question. Is the Department going to apply the SAFETY Act to the pharmaceutical industry when it comes to the development of biological countermeasures?

Answer. A very wide range of technologies may potentially qualify for protection under the SAFETY Act. The Act explicitly applies to any qualifying product, equipment, service (including support services), device, or technology (including information technology) that is designed, developed, modified, or procured for the specific purpose of detecting, identifying, preventing, or deterring acts of terrorism, or limiting the harm that such acts might otherwise cause. This broad definition of "technology" encompasses tangible products, software, services, various forms of intellectual property, and anything else that can be sold that has a specific anti-terrorism application. This definition of technology would encompass pharmaceutical products and their related delivery technologies when used for anti-terrorism purposes.

Question. How is S&T working with the drug and vaccine industry to determine which products should be considered for SAFETY Act protection?

Answer. The Office of Safety Act Implementation (OSAI) has a robust outreach program. Members of OSAI staff frequently provide informative presentations on the SAFETY Act at a variety of trade shows and industry meetings and often have a presence in the vendor areas where additional informative material on the application process and the benefits of protection under the SAFETY Act are available. OSAI staff members also provide informal guidance on an individual basis at these same events. In addition, OSAI will host another round of nationwide SAFETY Act seminars to introduce prospective applicants to the program including the benefits of SAFETY Act protections, the new application kit, and the revised interim rule.

The Department does not pre-determine if a particular technology is an anti-terrorism technology within the context of the SAFETY Act. Each applicant describes its specific anti-terrorism technology in its application and explains why it believes the technology or its proposed use of the technology meets the statutory criteria. OSAI does provide personalized guidance to applicants on a variety of issues at a number of points throughout the application process. Most often, the anti-terrorism application of the technology is reviewed, analyzed, and discussed with the applicant during the pre-application process, telephone discussions following receipt of the formal response to the pre-application, and through telephone conversations at the end of the completeness review before formal evaluation is commenced.

While we are not able to assess directly the extent to which this information has penetrated the pharmaceutical community, the fact that we have received some applications relating to vaccines indicates that some measure of penetration has been achieved.

Question. Is the SAFETY Act perhaps too limited with respect to certain areas? Is the Department reviewing the Act's authorities and issuing regulations or other administrative means to best utilize the Act?

Answer. The Department is committed to the primary goal of the SAFETY Act—to ensure that the threat of liability does not deter potential manufacturers or sellers of critical anti-terrorism technologies from developing and commercializing technologies that could save lives. The SAFETY Act review process is not intended to guarantee that anyone will be able to purchase "the very best" product or services. It is designed, as required by the statute, to help individual effective technologies overcome market barriers on an application-by-application basis. Throughout its implementation of this program, the Department has engaged applicants, industry, and the public to solicit feedback to enhance the process. Many concerns raised by interested parties have already been addressed and the Department will continue to encourage input to improve the program. The Department is committed to fulfilling the intent of Congress as set forth in the language of the SAFETY Act and will continue to improve upon efforts working towards successful implementation of this important legislation.

Among the efforts being undertaken by the Department to improve its implementation of the SAFETY Act are revisions to the application kit and the interim rule. The initial application kit was designed with the expectation that changes would be required as operational experience was obtained. During the past year, Office of Safety Act Implementation (OSAI) has sought input from applicants, industry, and government on areas appropriate for revision. Using this input and its own operational experience, OSAI prepared a revised application kit in concert with the proposed revision to the interim rule. The Paperwork Reduction Act notice for the final version of the new kit was published in the Federal Register on December 13, 2004. In addition, the Department is in the process of developing revisions to the current regulation. The revised regulations will address public comments and address other areas with a view to facilitating greater participation in the SAFETY Act program.

RAPID PROTOTYPING

Question. How does the rapid prototyping function within S&T assist in the Department's effort to combat bioterrorism?

Answer. The S&T Directorate's Rapid Prototyping Portfolio assists in the effort to combat bioterrorism by reducing the time needed to develop and commercialize relevant technologies that can meet needs on an interim basis while technologies that meet long-range needs are in development. The S&T Directorate's first rapid prototyping effort (conducted with the Technical Support Working Group (TSWG) in fiscal year 2003) produced thirteen separate efforts related to combating bioterrorism. When developed and completed, these efforts will provide such capabilities as: better methods to characterize biological backgrounds in facilities; methods for large-scale restoration of biologically contaminated urban areas; a low-cost, personal bio-decontamination system; a biological aerosol threat warning detector; direct detection assays for botulinum toxin; and improvements in biological detection systems.

The S&T Directorate's Rapid Technology Application Program (RTAP) has worked intensively with the DHS internal customers and field agents to identify their most urgent needs for countering bio threats. These needs will be published to the private sector in early summer 2005 with the goal of delivering the prototypes to those customers within 18 months of contract award.

Question. Do bioterrorism-related technologies lend themselves well to rapid prototyping?

Answer. All technologies, including technologies for bioterrorism countermeasures lend themselves well to rapid prototyping. Technologies needed to combat bio-terrorism range from near-term prototypes to extremely difficult long-term projects. Based on the expressed expectations of DHS customers, tactical concerns in the field dominate. They need technical capabilities to determine if a suspicious substance is a bio-agent or powdered sugar, other capabilities to tell them if an entire area is contaminated or not, and a fast, reliable method of definitive bio-agent identification. Technically effective isolation or containment of suspected bio-contaminants and improved protection of field personnel from bio hazards are cited often as developments needed in the short term.

In other areas, such as bioinformatics, forensics, bioassays for novel or engineered bio-agents, rapid prototyping must give way to careful, painstaking, long-term development.

Question. How do you determine which items are chosen for the rapid prototyping program?

Answer. The Rapid Technology Application Program annually conducts a series of meetings with DHS internal customers and field agents, and State and local responders to identify their highest priority needs for rapid prototyping developments.

These customers identify and prioritize their needs in any technical area. Within the constraints of technical feasibility, development time (no longer than 18 months), and available resources, their top priority rapid prototyping needs will be developed.

Question. Has the rapid prototyping effort incentivized both the scientific community and entrepreneurs to develop products?

Answer. Industry has been avidly interested in the S&T Directorate's solicitations. For example, the S&T Directorate's first rapid prototyping effort (with TSWG in fiscal year 2003) was valued at $60 million over 2 years and resulted in 94 contract awards for research and development work now underway. When developed and completed, these efforts will provide such capabilities as: better methods to characterize biological backgrounds in facilities, methods for large-scale restoration of biologically contaminated urban areas, a low-cost, personal bio-decontamination system, a biological aerosol threat warning detector, direct detection assays for botulinum toxin, and improvements in biological detection systems. There were more than 3,000 initial submissions for that solicitation. The DHS Rapid Technology Application Program, currently valued at $35 million is scheduled to release its first public, competitive, rapid prototyping solicitation in early Summer 2005 and a proportional strong response is expected.

Question. What is the most difficult hurdle when it comes to rapid prototyping?

Answer. The most difficult part of the rapid prototyping process is deriving meaningful customer requirements that are feasible, affordable, and have a high potential for actual deployment upon completion of development.

Question. Do antidote and vaccine development fall under the rapid prototyping effort or is that entirely under HHS' jurisdiction?

Answer. Section 302(4) of the Homeland Security Act of 2002 assigns to the Under Secretary for Science and Technology the responsibility for, . . . conducting basic and applied research, development, demonstration and testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that such responsibility does not extend to human-health related research and development activities:" [emphasis added]. Section 304 (a) assigns this responsibility to the Secretary of Health and Human Services.

Question. Are different tools combined and cross-pollinated to accelerate research and development when rapid prototyping to address bioterrorism?

Answer. Yes. The S&T Directorate's Rapid Prototyping development period is nominally between 6 and 18 months from contract award. In all but a very few cases this implies that most rapid prototypes will not involve basic research, but will heavily involve development. These developments take forms such as modifications of existing equipment for new purposes, increases in effectiveness derived from new algorithms or software, changes in configuration to be smaller, lighter weight, or redesign for decreased power consumption for example. Many of these rapid prototyping developments use "tools" developed for other purposes. Personal Data Assistants can be modified for identification of, and use by emergency responders. Personnel protective equipment can be redesigned to be less bulky, more effective against an array of hazards and more user-friendly. Wireless communications technology, for example, has many uses in bio countermeasures and it can be licensed off-the-shelf for many applications.

Question. How are the legal ramifications to rapid prototyping being addressed when S&T is dealing with items which do not have patents filed? Under this scenario, who owns the intellectual property when the product is changed as it moves through the rapid prototyping process?

Answer. In all but a very few cases most rapid prototypes will be heavily focused on late stage development. These developments take forms such as modifications of existing equipment for new purposes, increases in effectiveness derived from new algorithms or software, changes in configuration to be smaller, lighter weight, or have decreased power consumption, for example. The S&T Directorate will use procurement contracts (or Other Transactions for Prototypes) for rapid prototyping developments. Both kinds of vehicles are legally binding and require negotiation of many aspects of the development. Generally the developer retains title in any invention or data developed with the Government receiving a license. When appropriate, the Government will require licenses for Federal, State, tribal, and local government use. Specific intellectual property treatment, ownership, licensing, usage and royalties are always addressed in these detailed negotiations and contractually secured on terms agreeable to the developer and the Government, subject to all applicable laws and regulations.

QUESTIONS SUBMITTED BY SENATOR PETE V. DOMENICI

CHEMICAL AND BIOLOGICAL DETECTION PROGRAM

Question. In 2003, the Department of Energy transferred to the Department of Homeland Security a highly successfully Chemical and Biological Detection program, including $78 million in annual funding. This was a capability supported in conjunction with the nuclear detection capabilities at our national laboratories.

How much progress has DHS made in implementing this capability and how much is budgeted for these activities?

Answer. The Department of Energy's Chemical and Biological National Security Program (CBNP) was a highly successful R&D program that served as the foundation of the S&T Directorate's Biological and Chemical Countermeasures Portfolio, which was eventually split into biological and chemical components. The program was continued, augmented, and expanded to cover a range of biological and chemical countermeasures R&D targeted at homeland security applications. Efforts initiated in the CBNP that have come to fruition include the Biological Aerosol Sentry and Information System (BASIS), a deployable capability for biological threat agent detection that is now part of the S&T Directorate's special event monitoring and National Security Special Events (NSSEs), and served as the foundation for the BioWatch program that was deployed to over 30 U.S. cities. The Program for Response Options and Technology Enhancement for Chemical Terrorism (PROTECT) currently is operational and owned and operated by the Washington Metropolitan Area Transit Administration and the associated program in the San Francisco International Airport has provided guidance on airport protection. A restoration demonstration effort is underway there and will be completed this year. PROTECT served as a basis for the operational NSSE chemical protection efforts in New York City and Boston in fiscal year 2004.

Another key CBNP chemical defense program is the MicroChem lab, an effort to develop a next-generation hand-held chemical detector with capability to detect a broader set of chemical hazards than currently available sensors and with fewer false positive responses. Under DHS funding in fiscal year 2003 and fiscal year 2004, the effort has now completed development through prototype phase and will be evaluated against other developing sensors under the S&T Directorate's Chemical Detection program test/evaluation phase. There is no current active funding for this project as it has already accomplished the target prototype needed for evaluation. After fair test and evaluation among all candidates, successful technologies will be selected for further support toward final engineering. The Local Integration of NARAC (National Atmospheric Release Advisory Center) with Cities (LINC) program will continue to operate in its current configuration in five U.S. cities through this fiscal year and will be subsumed into the Biological Warning and Incident Characterization System once it is mature. R&D efforts that transitioned with the program in March 2003 have been continued through this year and new ones, such as the foreign animal disease R&D efforts and NBACC-related activities have been initiated. In fiscal year 2004, Biological Countermeasures was funded at $286.5 million and in fiscal year 2005, $362.6 million.

Question. Under the DHS Chem-Bio Detection program many research and development contracts have been made through industry instead of the national labs. The laboratory program supported a long term capability, but has also been successful in commercializing handheld detection units.

How is DHS allocating funding between industry, universities and national laboratories?

Answer. The S&T Directorate collaborates with academia through the Centers of Excellence program and its associated Integrated Network of Centers, which is establishing a national network of affiliated universities. Additionally, the S&T Directorate has a sizeable number of interactions and programs with individual universities on specific research topics and needs.

The S&T Directorate solicits proposals from industry and uses a full range of contracting vehicles and its authority under the Homeland Security Act to engage businesses (large and small), federally funded research and development centers, universities, and other entities in development of advanced technologies for homeland security. The contracted research and development work now underway is the S&T Directorate's main form of collaboration with industry and academia. The S&T Directorate maximizes and leverages the existing capability base of the national laboratory complex. The Directorate engages all the national laboratories on a case-by-case basis, to tap into unique technical expertise that is critical to accomplishing portfolio objectives and goals. The Directorate also relies on national laboratory technical experts as needed throughout the RDT&E processes based on their years

of experience applying technologies and processes to field applications. This technical and practical expertise is used to accelerate spiral development of technologies for transitioning capabilities to operational end-users.

The S&T Directorate's CounterMeasures Test Beds (CMTB) program operates in close partnership with a number of Federal and national laboratories to execute its mission of testing and evaluating all threat countermeasures and systems. The following national laboratories participate in all CMTB Operational Testing and Evaluation (OT&E) efforts and enable deployments in response to heightened alert conditions as necessary. Multi-laboratory teams are encouraged to ensure objectivity and a healthy interchange of ideas.

The Office of Interoperability and Compatibility (OIC) is currently leveraging the resources of Eastern Kentucky University in developing effective test methodologies for equipment and to provide technical assistance to states and localities under the SAFECOM Program. At the same time, OIC has enlisted a consortium of well over one hundred universities and colleges to support the annual conference on Technologies for Public Safety in Critical Incident Response, jointly sponsored by DHS and the Department of Justice (DOJ).

Industry associations participate in SAFECOM Program activities, especially in standards development efforts. OIC has established a monthly vendor process which allows for constant communication and collaboration with our industry partners. Additionally, OIC/SAFECOM will be conducting an industry summit in late fall to allow for ever greater collaboration.

Question. Is this allocation sufficient to support long term research and development necessary to develop the next generation technology?

Answer. The S&T Directorate's strategic planning process uses a risk-based approach (including threats, vulnerabilities, and consequences) that identifies critical areas of need for RDT&E. The potential impact of RDT&E investments is evaluated and those efforts, both short- and long-term, that will have the greatest impact on reducing risk are pursued.

In the 2 years that this Department has been in existence, the S&T Directorate has focused its efforts on near-term development and deployment of technologies to improve our Nation's ability to detect and respond to potential terrorist acts. However, we recognize that a sustained effort to continually add to our knowledge base and our resource base is necessary for future developments. Thus, we have invested a portion of our resources, including our university programs, toward these objectives.

The S&T Directorate believes the distribution of funding between industry, universities, and national laboratories supports both long-term capabilities development as well as meeting near-term requirements for end-users. The current funding distribution may change based on national requirements and needs. We recognize the value of longer-term capability development to ensure that the Nation has the necessary knowledge for application development.

Question. Can you please provide me list of the grants the Department has made in allocating the Chem-Bio diction funding for this the past year?

Answer. The fiscal year 2004 grants that DHS has made in the area of chemical and biological detection and related areas are listed below:

Performer	Topic
U of Pitt	Surveillance—RODS Decision Enhancements for The BioWatch System
Johns Hopkins	Surveillance—ESSENCE Implementation of ESSENCE Biosurveillance Systems
Arizona University	High Resolution DNA Signatures for biothreat
Multiple [1]	ECBC—Technical Advisory Group to HSARPA on Bioaerosol sensor testing and evaluation.
Multiple	Bioinformatics and Assay Development Program
Potomac Institute for Policy Studies	Bio-Alert
MIT/Lincoln Lab	Architecture Studies
Johns Hopkins University/APL	Real-Time Neutralization of Biological Weapons in Stadiums or Arenas
SAIC and Battelle	Demonstration & Verification of Chlorine Dioxide Decontamination Tech. in Large-Scale Test
National Center for Atmospheric Research	Urban Studies-Atmospheric Transport & Dispersion Calculations
MIT/Lincoln Laboratory	Water System Vulnerability Studies for Homeland Defense
Edgewood Chemical and Biological Command	Detection Systems for Biological and Chemical Countermeasures

Performer	Topic
MIT/Lincoln Laboratory	High-Collection-Efficiency Bio-aerosol Sampling
General Dynamics/CBRTA	DFU Filter Replacement Study
NYC DOHMH	Integration of Clinical Testing to Complement BioWatch and Disease Surveillance in NYC
Army Research Laboratory	Detection Systems for Biological and Chemical Countermeasures
Naval Research Laboratory	Detection Systems for Biological and Chemical Countermeasures
Battelle Laboratory	Detection Systems for Biological and Chemical Countermeasures
Ionian Corp	Detection Systems for Biological and Chemical Countermeasures
Johns Hopkins University/APL	Detection Systems for Biological and Chemical Countermeasures
Research Triangle Institute	Detection Systems for Biological and Chemical Countermeasures
Multiple	Detection Systems for Biological and Chemical Countermeasures
Agilent Corp	Detection Systems for Biological and Chemical Countermeasures
Smiths Detection/Pasadena	Detection Systems for Biological and Chemical Countermeasures
JHU/APL	Detection Systems for Biological and Chemical Countermeasures
Smiths Detection/Watford	Detection Systems for Biological and Chemical Countermeasures
Goodrich Corp	Detection Systems for Biological and Chemical Countermeasures
Sarnoff Corp	Detection Systems for Biological and Chemical Countermeasures
DOE National Laboratories	Enhanced Bioaerosol Detection System
Lawrence Livermore & Sandia Natl Laboratories	Bio-briefcase
Pacific Northwest Natl Lab	Botulinum detection system
Institute for Defense Analysis	IDA Chemical Hazard Analysis
Edgewood Chemical and Biological Command	Evaluation of Fielded Decontaminants Against Non-Traditional Agents
Institute for Defense Analysis	Infrastructure Sensitivity to Chemical Hazards
MITRE Corp	A JASON Study of Selected Topics for the Department of Homeland Security
Naval Research Laboratory	Detection Systems for Biological and Chemical Countermeasures use of CASPAR
Naval Research Laboratory	Autonomous Rapid Facility Chemical Agent Monitor
National Institute for Standards Technology	Solid State MEMs Microsensor Arrays to Detect Dangerous Chemicals
Goodrich Corp	TeraSpec
Sarnoff Corp	TeraSpec
Multiple	Detection Systems for Biological and Chemical Countermeasures
Monterey Institute	Survey/Evaluation of CBW Detectors
Multiple	Low Vapor Pressure Chemical Detectors
Los Alamos National Lab	Study of Receptor Development for Certain Chemical Threat Agents
Multiple	Novel Personnel Protection Equipment, BAA 04–13
Multiple	Bioinformatics and Assay Development Program
Lawrence Livernore Lab	Bioassays for Detection and Forensics
Los Alamos Nat'l Lab	Bioassays for Detection and Forensics
Sandia National Labs	Bioforensics
National Academy of Sciences	Assessing Vulnerabilities Related to the Nations Chemical Infrastructure
Scientific Applications International Corp	IBIS TIGER Biosensors
Space and Naval Warfare Command	Border Net (Chem/Bio Agent Support)
Naval Sea Systems Command	Chem/Bio Agent Support
Lawrence Livermore & other DOE Labs	High Throughput Diagnostics for Agricultural Applications
Palo Alto Sensor Technology Innovation	New System/Technologies to Detect Low Vapor Pressure Chemicals (e.g., TICs)

Performer	Topic
Seacoast Science, Inc	New System/Technologies to Detect Low Vapor Pressure Chemicals (e.g., TICs)
Intelligent Optical Systems, Inc	New System/Technologies to Detect Low Vapor Pressure Chemicals (e.g., TICs)
Synkera Technologies Inc	New System/Technologies to Detect Low Vapor Pressure Chemicals (e.g., TICs)
Cape Cod Research, Inc	New System/Technologies to Detect Low Vapor Pressure Chemicals (e.g., TICs)
CogniScent, Inc	New System/Technologies to Detect Low Vapor Pressure Chemicals (e.g., TICs)
Technispan LLC	New System/Technologies to Detect Low Vapor Pressure Chemicals (e.g., TICs)
Nanomat, Inc	New System/Technologies to Detect Low Vapor Pressure Chemicals (e.g., TICs)
Weld Star Technology, Inc	Chem-Bio Sensors Employing Novel Receptor Scaffolds
SomaLogic, Inc	Chem-Bio Sensors Employing Novel Receptor Scaffolds
Orthosystems, Inc	Chem-Bio Sensors Employing Novel Receptor Scaffolds
Nomadics, Inc	Chem-Bio Sensors Employing Novel Receptor Scaffolds
Peterson Ridge LLC (dba Fluence)	Chem-Bio Sensors Employing Novel Receptor Scaffolds
BioElectroSpec	Chem-Bio Sensors Employing Novel Receptor Scaffolds
Echo Technical	Chem-Bio Sensors Employing Novel Receptor Scaffolds
Operational Technologies Corporation	Chem-Bio Sensors Employing Novel Receptor Scaffolds
Accacia International LLC	Chem-Bio Sensors Employing Novel Receptor Scaffolds
BioTraces, Inc	Chem-Bio Sensors Employing Novel Receptor Scaffolds
CFD Research Corporation	Advanced Low Cost Aerosol Collectors for Surveillance Sensors and Personal Monitoring
Digital Flow Technologies, Inc	Advanced Low Cost Aerosol Collectors for Surveillance Sensors and Personal Monitoring
MesoSystems Technology Inc	Advanced Low Cost Aerosol Collectors for Surveillance Sensors and Personal Monitoring
Research International, Inc	Advanced Low Cost Aerosol Collectors for Surveillance Sensors and Personal Monitoring
InnovaTek, Inc	Advanced Low Cost Aerosol Collectors for Surveillance Sensors and Personal Monitoring
Enertechnix, Inc	Advanced Low Cost Aerosol Collectors for Surveillance Sensors and Personal Monitoring
Isotron Corporation	Wide-Area TIC Neutralization
Gumbs Associates, Inc	Wide-Area TIC Neutralization
Synergistic Advanced Technologies LLC	Wide-Area TIC Neutralization

[1] Multiple indicates contract awards to more than one recipient in a category from the funding provided for this solicitation. In most cases, there remain companies in negotiation for award.

QUESTIONS SUBMITTED BY SENATOR ROBERT C. BYRD

CHEMICAL DETECTORS

Question. In your oral testimony, you indicated that there are funds in the budget to deploy chemical sensors, yet the S&T budget document refers to "critical design review" of technologies, but nothing about deployment of sensors across the country. Based on your hearing comments, please provide specifics on the Department's capabilities and deployment schedule for chemical monitoring.

Answer. The interface to which this question refers was a short discussion on the issue of PROTECT, a networked chemical detection system for enhanced response against chemical attacks on facilities, particularly transit systems. This system has been demonstrated in and transitioned to three subway systems (DC, Boston, and NYC). With successful demonstration, the program has transitioned away from DHS S&T Directorate and is available for installation in other transit systems via the fiscal year 2005 Transit Security Grants Program administered by the DHS Office of State and Local Government Coordination and Preparedness (SLGCP) Office for Domestic Preparedness. The reference to "funds in the budget" to support deployment was a reference to funds in the Department's budget versus the S&T Directorate budget. The fiscal year 2005 Transit Security Grant Program includes $108 million for rail transit security, targeted to specific urban areas for the prevention and detection of explosive devices and chemical, biological, radiological and nuclear agents. Expenditures to acquire the PROTECT system are permissible under this

program. The Science and Technology Directorate is assisting SLGCP with technical data package development and is prepared to offer technical assistance in the deployment of the system through this program.

BIOWATCH DETECTION

Question. Your budget proposes over $100 million for bio-aerosol detection systems, better known as the "BioWatch" program. These sensors are located in over 30 major cities across the country.

Samples are taken manually 1 or 2 times daily and then tested at a lab to determine if a biological attack has occurred. If an attack really occurs, hundreds or thousands of people could be harmed before the lab results come in. What investments are you making to close the gap between the release of a biological agent and the time it takes to detect it?

Answer. We have a major program to develop the next generation of biodetection systems which we call Biological Autonomous Networked Detection (BAND). These systems will collect and analyze the sample on site, reporting out as often as every four hours, and will wirelessly transmit the data from any positives to the nearest Laboratory Response Network for confirmation and to initiate sample retrieval. The BAND system will simultaneously perform analyses for twenty or more agents, significantly more than the current BioWatch system, with sensitivities and false alarm rates equal to or better than the current BioWatch system. Because the sample collection and analyses is fully automated and done on site, the operational costs per "detection site" will be about one-fifth that of the current system or less. This greatly lower operational cost and the fully autonomous nature of the system will enable expansion of biological protection within existing BioWatch cities as well as to those cities and venues where it was previously not practical. We are currently on schedule for demonstrating a laboratory prototype of the BAND system in fiscal year 2006, developing engineering prototypes in fiscal year 2007, piloting them in a BioWatch city or cities in fiscal year 2008 and deploying them throughout the existing BioWatch cities in fiscal year 2009/fiscal year 2010.

Question. My understanding is that certain prototypes are being tested, but they won't be deployable until 2009. Is this a matter of resources? What is needed to accelerate deployment of this system?

Answer. Your understanding is correct, as per the discussion previously, we are not scheduled to begin deployment of the BAND System to BioWatch cities until fiscal year 2009. This is in part technology limited and in part resource limited. If the available R&D funding for this system was increased from its projected fiscal year 2006-fiscal year 2007 levels of about $25 million per year to $60 million per year, we would be able to significantly reduce the technical risk in developing the system and speed its deployment by 6 to 12 months. This would be accomplished by pursuing more technology options more aggressively. The competition engendered by being able to carry two or three systems all the way through development would further assist in meeting the challenging technical performance and cost goals. In addition, manufacturing of these detection systems to enable wide scale deployment would benefit from creating a guaranteed market for 1,000–2,000 of these advanced detection systems, at a total estimated cost of $50–100 million. A significant portion of this additional required funding would need to be available in fiscal year 2007 so as to enable deployment to start in fiscal year 2008.

BIOWATCH RESPONSE

Question. The budget notes as an accomplishment that the "BioWatch" detection systems, which are deployed in over 30 major U.S. cities, conducted over a million assays with no false alarms.

While that is certainly an indication that the system works, an official with the National Association of County and City Health Officials recently complained that not enough focus has been placed on what happens if the "alarm bell" rings.

If an incident of national significance is detected, are State and local governments prepared to respond?

Answer. The S&T Directorate, in collaboration with CDC, EPA, and DoJ, has prepared BioWatch Preparedness and Response Guidance (interim draft guidance) and distributed it to the BioWatch cities. This draft guidance is intended to assist the cities in their development of an incident characterization plan following a positive BioWatch signal. While some cities have developed a comprehensive plan, other cities' plans are under development. The S&T Directorate continues to offer assistance to each city and currently has an effort underway to address the concerns of the local public health epidemiology community.

Question. What management practices are in place at the Federal level to ensure that State and local governments are prepared to respond to an incident of national significance? I would like to hear both Assistant Secretary Albright and Assistant Secretary Simonson respond to the question.

Answer. Contingency planning with State and local governments is an important and ongoing process. A key component of the National Incident Management System (NIMS) compliance for State and local jurisdictions is the requirement for updating and revising emergency operations plans. With the release of the National Response Plan (NRP), State and local jurisdictions are encouraged to align their plans with the NRP. State, local, and tribal organizations must adopt NIMS by fiscal year 2007 as a condition of receiving Federal preparedness assistance. State and local governments can use DHS grant funds to implement the NIMS.

The NRP and the NIMS provide the template, policies, and protocols for integrating all jurisdictions and the private sector as key components of the Nation's response to domestic incidents. The NRP and the NIMS are built on the principle that most incidents start, end, and are managed at the local level. The NIMS stresses the concepts of mutual aid, communications, resource typing, and preparedness, in addition to the command and control elements, including the Incident Command System and Multi-agency Coordination. The NRP details how those varying levels of responsibility work together during Incidents of National Significance (a new concept developed in the NRP to cover every significant incident), which require the Department of Homeland Security to take on the overall coordination role for Federal involvement in domestic incident management. The NRP provides the multi-agency coordination structures to support incident commanders and local entities at the scene. It also provides coordination structures for integrating with the private sector. One of the key concepts of the NRP is that preventing, preparing for, responding to, and recovering from Incidents of National Significance require the collective capabilities of all involved jurisdictions.

DOMESTIC NUCLEAR DETECTION OFFICE (DNDO)

Question. The DHS budget proposes $227 million for a new office called the Domestic Nuclear Detection Office (DNDO). I share the Department's concerns that this threat warrants a coordinated effort at the Federal level to address it. However, the criticism following 9/11 that led to the creation of the Department of Homeland Security was that there were too many stovepiped agencies across the Federal Government dealing with homeland security that didn't know what the other was doing.

In your opinion, is enough being done by the Secretary's office to ensure that the DNDO will not become a stovepiped organization?

Answer. One of the principal motivators in the formation of the DNDO was to remove this type of stovepiping within the Department, and across the Federal Government, with regards to the prevention of nuclear terrorist attack. DNDO is charged with integrating and coordinating all planning and implementation efforts across the other Federal departments and agencies, and within DHS, to ensure that individual efforts are effectively and efficiently contributing to a global strategy to defend against the terrorist use of a nuclear weapon on our Nation.

The DNDO serves as a unique entity within the Department to consolidate all nuclear-detection related activities, allowing for the development of an integrated office that will be responsible not only for research and development, but also for developing a global nuclear detection architecture and developing and implementing a domestic detection system, to include acquisition programs for detection assets and operational support functions. This integration, as well as coordination with nuclear detection programs in other departments, will allow for the development of a single global nuclear detection architecture to protect the Nation from attempts to import or transport a nuclear device or fissile or radiological material intended for illicit use.

Question. For instance, the proposal for DNDO calls for its own office of assessments and evaluations. It has its own policy planning office. It has an R&D office as well as a systems development and acquisitions office. These are also functions currently performed by the Science and Technology Directorate and the Information Analysis and Infrastructure Protection (IAIP) Office.

Is the Secretary proposing to set up a separate intelligence unit and a separate R&D arm just for this office? How does this affect ongoing efforts within the Science & Technology Directorate?

Answer. With regards to intelligence collection and analysis, IAIP will continue to be the conduit for DNDO coordination with the larger intelligence community. Additionally, DNDO will leverage the current capabilities within IAIP for intelligence analysis. The DNDO's Joint Center for Global Connectivity (JCGC) will be

closely integrated with the Homeland Security Operations Center (HSOC) to ensure that effective information flows in both directions. DNDO expects to receive all relevant intelligence information from IAIP in a timely manner and will provide additional technical analysis capabilities on a 24/7 basis as part of the JCGC. The JCGC, by receiving information and finished intelligence from sources across the Federal, State and local levels, will be able to additionally provide continuous analysis of real-time data streams and the capability to provide continual national situational awareness.

With regards to research and development, the DNDO will continue to closely interface with the S&T Directorate on joint projects, as appropriate, for the development of technologies that may provide countermeasures against multiple threat types. The separation of the DNDO nuclear detection research, development, test, and evaluation (RDT&E) from the RDT&E conducted within the S&T Directorate will be conducted so as to not have any detrimental affect on potential collaborative efforts that would be gained through the S&T consolidation effort. The goal is to make sure that this Nation maintains a preeminent research and development program to address the technical challenges in radiation detection science and technology, while at the same time capitalizing on the benefits of integrating this program with larger acquisition and operational support efforts.

Again, the intent of the DNDO is to provide an integration of efforts across the Department, as well as the rest of the Federal Government, rather than another disconnected layer of bureaucracy. For exactly this reason, the DNDO will be a jointly-staffed office with detailed employees from other DHS components, as well as other departments, to provide strong linkages and a mutual continual awareness between the DNDO and the parent organizations. The DNDO will not operate in a vacuum separate from the rest of the Department, but will instead operate in a fully-informed environment, cognizant of all relevant Department efforts, including the intelligence and R&D efforts mentioned.

RADIOLOGICAL/NUCLEAR COUNTERMEASURES TEST AND EVALUATION COMPLEX

Question. The budget request includes $9 million for a Radiological/Nuclear Countermeasures Test and Evaluation Complex. The budget indicates that $13 million was appropriated prior to fiscal year 2004 and $11 million was appropriated in fiscal year 2004. When was the $13 million appropriated? Under which public law or laws was the funding included?

Answer. At the stand up of DHS and S&T, funds were transferred from other departments to provide an initial funding base. In particular, funds for the Radiological/Nuclear Countermeasures Portfolio were originally transferred from the Defense Threat Reduction Agency (DTRA) and the Department of Energy (DOE). The first $13 million that was put on contract for the Radiological/Nuclear Countermeasures Test and Evaluation Complex was part of the fiscal year 2003 funding. Funding was included under a reprogramming of funds request, and Radiological/Nuclear Countermeasures received $65 million which was approved by the House and Senate Appropriation Committees. The reprogramming did not specifically state that the S&T Directorate was using funds for the Radiological/Nuclear Countermeasures Test and Evaluation Complex; however, the S&T Directorate used $13 million for this effort.

Question. The project schedule indicates that the construction phase is scheduled to begin on May 1, 2005. Is the project on schedule? If not, what impact does that have on the June 2006 completion goal?

Answer. The Radiological/Nuclear Countermeasures Test and Evaluation Complex (CTEC) construction project is currently on schedule to meet the expected June 2006 completion goal.

UNIVERSITY CENTERS OF EXCELLENCE

Question. Under Secretary McQueary testified last year that in addition to the risk analysis and agro-terrorism centers, two more solicitations would occur in fiscal year 2004 and if the budget request for fiscal year 2005 was maintained at fiscal year 2004 levels, an additional five Centers could be selected for a total of nine centers. In fiscal year 2005, the fourth center was named, but the fiscal year 2006 budget request indicated that a fifth is being evaluated and two additional Centers are anticipated in fiscal year 2005 and fiscal year 2006 for a total of seven.

Why has the number of Centers planned by the Department changed?

Answer. The Science and Technology Directorate plans on supporting seven Centers of Excellence and two Cooperative Centers in fiscal year 2005 and fiscal year 2006, for a total of 9 Centers supported. The Broad Agency Announcement (BAA) for the fifth Center had proposals due at the end of April 2005. The BAAs for the

sixth and seventh Centers are in development. The DHS–EPA Cooperative Center on Microbial Risk Assessment has been funded for fiscal year 2005, with the recipient to be announced shortly, and the second Cooperative Center is in development.

Question. What areas of mission relevant research are not being considered because of the reduction from nine to seven Centers?

Answer. We are planning on supporting a total of seven merit-based Centers of Excellence through fiscal year 2006; topics for the sixth and seventh Centers are being vetted within the Department for approval prior to announcement. We anticipate releasing Broad Agency Announcements requesting proposals for merit-based consideration in fiscal year 2005. In addition to the seven Centers of Excellence, the S&T Directorate will support two Cooperative Centers in fiscal year 2005 and fiscal year 2006. We believe that these seven centers will address all current mission relevant research.

NATIONAL BIO AND AGRODEFENSE FACILITY

Question. The budget proposes $23 million for the National Bio and Agrodefense Facility, which according to the project schedule, will cost over $450 million to complete. According to the project schedule, work to be performed in fiscal year 2006 will cost only $3 million. Why is $23 million needed in fiscal year 2006?

Answer. The $3 million referenced will be spent in fiscal year 2005 to initiate a conceptual design study to define the scope and size of the new facility. The $23 million fiscal year 2006 request will complete the conceptual design, the NEPA process including site selection, and initiate the detailed engineering design of the chosen concept.

Question. Has a site been selected for this facility?

Answer. No site has been chosen at this point in the NBAF development process. An interagency conceptual study has been undertaken by DHS, USDA and DHHS to explore three major options for NBAF each with increasing capability. The study will determine the programmatic requirements, scope and size of the facility taking into account cost, schedule, technical requirements and public support. This process will provide the basis for more detailed engineering design, NEPA evaluation and the site selection.

Question. Is an authorization required for this facility?

Answer. It is our understanding that under current legislation, an authorization for this facility is not required. However, should Congress decide to require one, we would of course comply.

CHEMICAL COUNTERMEASURES

Question. The budget request includes an additional $49 million for the chemical countermeasures portfolio. The request indicates that $24 million supports construction of a new facility for countermeasures testing. The object class for this funding is listed under "Purchase of goods/services from Gov't accounts." Will this facility be leased or owned by DHS? Where will it be located? Why isn't this facility listed under the Capital Investment and Construction Initiative Listing?

Answer. The budget request identifies a $24 million increase from fiscal year 2005 to fiscal year 2006 in "Purchases from Government Accounts." This funding includes support of two activities: construction of a singular facility to conduct tests of countermeasures against non-traditional agents and the enhancement of threat characterization, analysis, and assessment, including initiation of toxicology and environmental fate studies of non-traditional agents. For clarity, of this $24 million, only $11 million are apportioned to support the construction of the countermeasure test facility. The test facility will be constructed at Edgewood Area, Aberdeen Proving Ground, MD, and will be a Department of Defense (DOD) facility. The DHS funds will be utilized to conduct a series of critical studies to provide much of the foundation data to support design and safe use of the facility, which is required for countermeasures assessment both by DOD and DHS. A Memorandum of Agreement (MOA) between DHS and DOD is in development to outline agreement on the requirements, shared expenses, and use terms of the facility. Since the DHS funding is provided to another government agency (Army) to support a facility of that agency, the object class is identified as "Purchase of goods/services from Gov't accounts" versus Capital Investment.

QUESTIONS SUBMITTED TO STEWART SIMONSON

QUESTIONS SUBMITTED BY SENATOR JUDD GREGG

HEALTH AND HUMAN SERVICES AND BIOSHIELD

Question. Please provide a list of administrative, regulatory or legislative proposals needed to invigorate scientific research relevant to the development of needed countermeasures and products for natural pandemics and epidemics.

Answer. There is a very active scientific effort underway to develop needed medical countermeasures and products for natural pandemics and epidemics. Much of this effort is supported by the National Institute of Allergy and Infectious Diseases (NIAID) at the National Institutes of Health (NIH). For example, NIAID is using Project BioShield authorities to expedite the development of assays to be used for the high-throughput screening of candidate therapeutics for influenza. Influenza is currently considered a Category C biological threat agent by the Centers for Disease Control and Prevention (CDC). The influenza antiviral therapeutics currently available are limited and the rapid emergence of antiviral resistance with widespread use of these therapeutic agents is a potential concern.

Finding new options for treating influenza are a high priority for the Nation, as the Department of Health and Human Services (HHS) draft Pandemic Influenza Response and Preparedness Plan articulates.[1] Grants will support research projects focused on the development of needed diagnostic assays and screening techniques to permit speedier identification of compounds with the potential to be effective against a broad spectrum of influenza strains, including newly emergent influenza strains.

In an effort to address the pressing need for additional reliable influenza medical countermeasures, the RFP, NOT–AI–05–045, was released on June 17, 2005, and the receipt date for applications is September 1, 2005. Grants are expected to be awarded in fiscal year 2006. The Department of Health and Human Services will implement appropriate administrative and regulatory actions to facilitate this research activity.

Question. Many innovators complain that they cannot get access to your office for an evaluation of their new product ideas. Please describe your process for screening new products and new ideas.

Answer. HHS/OPHEP/ORDC has hosted numerous meetings with external stakeholders. These meetings provide a forum for innovators to give presentations on their products and to describe their capabilities to ORDC. We have had over thirty contacts from industry since January 2005. ORDC hosts a Project BioShield website http://www.hhs.gov/ophep/bioshield/ that provides frequently updated information on ongoing and planned acquisitions under Project BioShield. The website also has an email link that allows users to send a message directly to ORDC.

New products or ideas are screened depending upon factors including the credibility and potential impact of the threat it proposes to treat and stage of development in the research and development pipeline.

If the product is in the early stages of development, companies and researchers need to seek NIH funding through grants, contracts, partnerships or the Small Business Innovation Research (SBIR) program. The SBIR is a set-aside program (2.5 percent of an agency's extramural budget) for domestic small business concerns to engage in Research/Research and Development (R/R&D) that has the potential for commercialization. The SBIR program was established under the Small Business Innovation Development Act of 1982 (Public Law 97–219), reauthorized until September 30, 2000 by the Small Business Research and Development Enhancement Act (Public Law 102–564), and reauthorized again until September 30, 2008 by the Small Business Reauthorization Act of 2000 (Public Law 106–554).

If an innovator's product is sufficiently advanced in development, then the Office of Research and Development Coordination (ORDC) in the Office of Public Health Emergency Preparedness (OPHEP) at HHS meets with developers to provide guidance concerning the Project BioShield acquisition process. This process includes a Material Threat Determination (MTD) and a Material Threat Assessment (MTA) by the Department of Homeland Security. A MTD is issued by the Secretary of Homeland Security if it is determined that the specific CBRN threat presents a material threat against the United States population sufficient to affect national security. The MTAs provide information about the extent of the threat and the vulnerabilities and are used to inform U.S. Government (USG) medical countermeasure requirements. The USG requirements and recommendations for acquisitions are estab-

[1] A copy of the Pandemic Influenza Response and Preparedness Plan can be found at http://www.hhs.gov/nvpo/pandemicplan/.

lished by the interagency Weapons of Mass Destruction Medical Countermeasures Subcommittee of the National Science and Technology Council. The Project BioShield acquisition process also includes a joint recommendation for acquisition by the Secretaries of HHS and the Department of Homeland Security (DHS), and an approval for the acquisition by the White House.

Question. Several recommendations have been made to formalize access for screening new ideas for products, including convening a working group of outside experts, contracting with the private sector, and web-based submissions. Please provide a list of proposals on how you would recommend formalizing access for screening new ideas for products.

Answer. The NIH peer review process works very well in providing an initial evaluation of new ideas. Both NIH and ORDC staff frequently meet with developers using a "Technology Watch" process aimed at ensuring that USG medical countermeasure research and development experts are informed about promising, innovative products. As part of the Technology Watch process, ORDC issues periodic Requests for Information (RFI) to determine the level of maturity of the medical product targeting countermeasures of interest in the developmental pipeline. Finally, ORDC has a regularly updated website and an email address that allows for web-based submission of questions.

Question. You made mention in your testimony of a number of Project BioShield related procurement-related activities that include Pre-solicitation notices, Requests for Information, and Requests for Proposals. Can you provide additional information about these activities?

Answer. A copy of the current OPHEP/ORDC BioShield procurement activities is attached for your convenience. Furthermore, information on these procurement-related activities is available on our website at http://www.hhs.gov/ophep/bioshield/PBPrcrtPrjct.htm. This information is also available at http://www.fedbizopps.gov.

Question. As described in the Project BioShield Act of 2004, there are a number of determinations that must be made to support the acquisition of a security countermeasure using the special reserve fund appropriated in the fiscal year 2004 DHS Appropriations bill. Can you please describe the role of HHS and the process used to make these determinations, specifically that the determinations that countermeasures are necessary and are appropriate for inclusion in the Strategic National Stockpile and the joint recommendation for procurement?

Answer. The Secretary of Homeland Security is charged with making material threat determinations (MTDs). Upon receipt of the DHS MTD the Secretary of Health and Human Services determines if medical countermeasures are necessary to protect the public health. If countermeasures are needed, the Secretary of Health and Human Services must determine the number of doses required, if production and delivery of a approved or licensed product is feasible with 8 years of contract award, and an evaluation of whether there is a commercial market for the product(s) other than as a security countermeasure. Finally, the Secretaries of Homeland Security and Health and Human Services jointly recommend to the President that the Special Reserve Fund be made available for the recommended countermeasure procurement. The approval for the procurement is made by the President (now delegated to the Office of Management and Budget.)

Question. In your testimony, you've provided us with a summary of the many accomplishments of your office since the enactment of the Project BioShield Act of 2004, also known as BioShield I. As you know, I am sponsoring the so-called "BioShield II" bill to further expand on the efforts of BioShield I including indemnification for product manufacturers and liability protection for health workers and patent protections. Do you feel that the new bill appropriately addresses remaining obstacles to medical countermeasure development against weapons of mass destruction?

Answer. The Department of Health and Human Services is committed to the development and acquisition of priority security countermeasures and will work with Congress and stakeholders to address obstacles to the effective implementation of Project BioShield.

Question. It is often stated that it takes 10 years to develop medical products. What makes HHS believe that it can accomplish this in less time?

Answer. It generally takes 10 years to develop a medical product from inception to full FDA licensure or approval by proceeding along a conservative, serial regulatory path. Project BioShield allows for the procurement and delivery of medical countermeasures to the Strategic National Stockpile (SNS) prior to full FDA approval or licensure and their use under the Emergency Use Authorization provision of the Project BioShield Act of 2004.

In order to acquire these critical medical countermeasures as quickly as possible, Project BioShield encourages a parallel development process in which the developer

concurrently is finalizing a formulation while conducting animal or human clinical trials and scaling up and validating a current Good Manufacturing Practices (cGMP) production process. This approach has some increased risk of failure; however, the process is very closely monitored by relevant HHS staff.

Question. There are many different biological threats. Can you explain why so much of the BioShield activities are focused on anthrax?

Answer. The initial focus of our efforts to protect the Nation was aimed largely at those threats that could do the greatest harm to the greatest number of our citizens—namely, smallpox and anthrax. An attack involving the aerosol dissemination of anthrax spores, particularly in an urban setting, was considered by public health experts to have the potential for catastrophic effects. The potential for large-scale population exposure following aerosol release of anthrax spores, the threat demonstrated by the anthrax letters, the persistence of anthrax spores in the environment and our knowledge that anthrax had been weaponized by state-actors, highlighted the nature of the threat. The Secretary of Homeland Security determined that anthrax posed a material threat against the United States population sufficient to affect national security. And, because untreated inhalation anthrax is usually fatal, the Secretary of HHS determined that additional countermeasures were necessary to protect the public health.

Question. I understand that the NIAID rPA anthrax vaccine advanced development contracts with VaxGen and Avecia are still ongoing. Why did you make the decision to commit to the acquisition of 75 million doses of this product before those NIAID contracts were completed?

Answer. The material threat assessment provided by the DHS supported the requirement to acquire sufficient vaccine to protect 25 million persons (75 million doses). The development work performed under the NIAID contracts had proceeded to a level such that HHS had confidence that a final rPA vaccine product was achievable and licensable within 8 years of a contract award.

Question. In your statement you testified that the stockpile already contains sufficient smallpox vaccine to protect every American. Can you please explain why it is necessary to purchase any additional vaccine?

Answer. The smallpox vaccines currently in the Strategic National Stockpile are live virus vaccines derived from a virus called vaccinia. These replicating vaccines are contraindicated in some segments of the population, particularly those with weakened immune systems. Therefore, there is a need to develop a vaccine which will be more appropriate for use in these persons. An attenuated smallpox vaccine with limited replication in humans, such as the Modified Vaccinia Ankara (MVA) vaccine would be appropriate for use in such individuals.

Question. Former Secretary Tommy Thompson stated that food-borne bioterrorism was one of his greatest concerns. Certainly, deliberate contamination of food with botulism could result in a large number of casualties. Would you please further describe your planned procurement for botulism countermeasures?

Answer. Botulism toxin was determined to be a material threat by the Department of Homeland Security on June 9, 2004. Presidential approval for the acquisition of botulinum antitoxin using special reserve funds under Project BioShield was granted on August 17, 2004. HHS released a presolictiation notice on September 4, 2004 indicating its intention to acquire 200,000 doses of heptavalent equine botulinum antitoxin through a sole-source contract. The Request for Proposal was issued to the prospective offeror on July 14, 2005. Horses are currently being immunized to generate the plasma necessary to produce the botulinum antitoxin. A contract award is anticipated in the 3rd quarter of 2005.

Question. There is concern that we may not be responding adequately to the threat of nuclear or radiological terrorism. What is HHS doing to protect the public from illness after exposure to radiation? Particularly, would you provide more information regarding procurement of medical countermeasures against this threat?

Answer. The Strategic National Stockpile (SNS) currently contains medical countermeasures to treat the spectrum of potentially life-threatening effects of radiation exposures. These include drugs to block entry or to remove radioactive particles from the body as well as to treat a major effect of penetrating radiation known as acute radiation syndrome (ARS). Specifically, the SNS currently contains the following:

—Potassium Iodide and a pediatric liquid formulation of potassium iodide. Potassium Iodide is used to block the uptake of radioactive iodine that could be released following a nuclear detonation or a nuclear power plant accident;

—Calcium and zinc diethylenetriaminepentaacetate (Ca/Zn DTPA). The DTPAs are used to remove radioactive transuranic particles such as plutonium and americium from the body following the use of a dirty bomb or similar device;

—Prussian Blue. This drug is used to remove radioactive cesium from the body after a nuclear detonation or use of a dirty bomb or similar device; and
—Filgrastim. This drug is used to treat life-threatening suppression of infection-fighting white blood cells after whole-body exposure to high doses of penetrating radiation—a form of acute radiation syndrome.

Additionally, a Request for Information (RFI) for countermeasures for an acute radiation syndrome was published in October 2004. Responses to that RFI have been evaluated and a Request for Proposals (RFP) is being developed. We are in the process of determining what the specific requirements and acquisition options are so that we can proceed with the acquisition process. HHS is eager to enlarge the holdings of the Strategic National Stockpile (SNS) with respect to radiological/nuclear countermeasures. Accordingly, the quality of the proposals and the stage of product development will determine how HHS acts on the results of the RFI and RFP.

Question. Nuclear or radiological terrorism has been cited as one of the greatest threats this country faces with regard to homeland security. Several promising bone marrow protection drugs could be available in the near term to protect against this threat. When do you expect to procure such drugs for the National Strategic Stockpile?

Answer. The Strategic National Stockpile (SNS) currently contains medical countermeasures to treat the spectrum of potentially life-threatening effects of radiation exposures. These include drugs to block entry or to remove radioactive particles from the body as well as to treat a major effect of penetrating radiation known as acute radiation syndrome (ARS). Specifically, the SNS currently contains the following:

—Potassium Iodide and a pediatric liquid formulation of potassium iodide. Potassium Iodide is used to block the uptake of radioactive iodine that could be released following a nuclear detonation or a nuclear power plant accident;
—Calcium and zinc diethylenetriaminepentaacetate (Ca/Zn DTPA). The DTPAs are used to remove radioactive transuranic particles such as plutonium and americium from the body following the use of a dirty bomb or similar device;
—Prussian Blue. This drug is used to remove radioactive cesium from the body after a nuclear detonation or use of a dirty bomb or similar device; and
—Filgrastim. This drug is used to treat life-threatening suppression of infection-fighting white blood cells after whole-body exposure to high doses of penetrating radiation—a form of acute radiation syndrome.

Additionally, a Request for Information (RFI) for countermeasures for an acute radiation syndrome was published in October 2004. Responses to that RFI have been evaluated and a Request for Proposals (RFP) is being developed. We are in the process of determining what the specific requirements and acquisition options are so that we can proceed with the acquisition process. HHS is eager to enlarge the holdings of the Strategic National Stockpile (SNS) with respect to radiological/nuclear countermeasures. Accordingly, the quality of the proposals and the stage of product development will determine how HHS acts on the results of the RFI and RFP.

Question. It is estimated that one quarter of the U.S. population cannot take the current smallpox vaccine that we have in our stockpile. NIH has been hard at work on the development of a safe MVA-based smallpox vaccine for that portion of the population that is contraindicated. Please describe where we are in the development of the vaccine and when you plan to issue your RFP for the purchase of the MVA vaccine?

Answer. HHS released a presolicitation notice in anticipation of releasing an RFP by the end of the summer to manufacture and deliver to the SNS up to 20 million doses of the attenuated smallpox vaccine, modified vaccinia Ankara (MVA).

Question. If the recent anthrax incident at the DC postal and DOD facilities had turned out be a real anthrax attack requiring the use of both antibiotics and the vaccine for those exposed and vaccinations for first responders, how many doses of the FDA licensed anthrax vaccine that are currently in Strategic National Stockpile managed by HHS would be used?

Answer. The SNS currently contains sufficient antibiotics to treat about 180,000 symptomatic anthrax patients and to provide for a 60 day prophylaxis of more than 25 million persons. This stockpile of antibiotics is growing monthly. The USG is currently negotiating for the acquisition of specific anthrax antitoxins to treat symptomatic anthrax patients. In addition to the use of antibiotics, HHS would deploy as much anthrax vaccine from the SNS as was required to respond to the event and to protect the population. The vaccine and the prophylactic antibiotics would likely be used concurrently. There currently is no FDA-licensed vaccine for post-exposure use following anthrax exposure. In May 2005, HHS awarded a contract to BioPort Corporation for the manufacture and delivery of 5 million doses of licensed anthrax vaccine adsorbed (AVA) to the stockpile. There are at present over 1 million doses

of AVA available for the pre-exposure immunization of at-risk groups such as certain laboratory workers and first responders who would be involved with the response to an attack.

Question. For the past 1½ years, HHS has been in the process of acquiring 5 million doses of the FDA licensed vaccine for the CDC stockpile while the agency has committed nearly $1 billion under government contracts to acquire 75 million doses of an early-stage anthrax vaccine from a single manufacturer. Why has it taken so long after the 2001 anthrax attacks for HHS to acquire any additional doses of the current FDA-licensed vaccine for the stockpile?

Answer. HHS acquired a small amount of the AVA vaccine for civilian use (21,400 doses) following the anthrax events of the fall of 2001. Thereafter HHS initiated a process to acquire licensed AVA anthrax vaccine from DOD. Various administrative and legal issues caused delays in this acquisition. Once Project BioShield was enacted, HHS determined that initiating a BioShield acquisition contract directly with the AVA vaccine manufacturer, BioPort Corporation, would be the best mechanism to acquire this vaccine. HHS awarded the contract on May 5, 2005 for 5 million doses and the company completed the initial delivery of over 1 million doses soon after contract award. We would be happy to provide timelines if helpful.

Question. Please explain the decision to eliminate from the President's fiscal year 2006 budget the funding for the CDC dose reduction studies to allow FDA approval for fewer doses of the FDA-licensed anthrax vaccine given that FDA approval of the new anthrax vaccine is still years away? If the number of doses for pre-exposure vaccinations against anthrax could be reduced in half, wouldn't that also result in significant net cost savings for the Federal Government and double the number of 1st responders and other who could be vaccinated and protected before an anthrax occurs?

Answer. At the inception of this program in 1999, HHS anticipated it would take 5 years to complete the necessary studies. It is important to note that this type of study is normally undertaken by the manufacturer in the interest of improving product utilization. To date the program has generated sufficient data to allow BioPort to submit a request to the FDA to change the route of administration from subcutaneous to intramuscular and to decrease the six dose priming series from six to five doses.

CDC has now completed the anthrax vaccine clinical trial interim safety analysis, has presented the results to key stakeholders and has submitted the final report detailing all findings from the safety analysis to the Food and Drug Administration (FDA). Accordingly, the HHS bioterrorism preparedness budget placed the highest priority on expanding mass-casualty treatment capacity and procuring additional pharmaceuticals for the Strategic National Stockpile.

Question. Would HHS provide assurance that the human clinical, animal and CDC laboratory dose reduction studies for the currently licensed anthrax vaccine will be continued and completed given the potential rapid deployment and cost saving benefits for first responders, lab workers and others from fewer doses?

Answer. Yes. As indicated above, HHS anticipated it would take 5 years to complete the necessary studies. CDC has now completed the anthrax vaccine clinical trial interim safety analysis. The program has generated sufficient data to allow BioPort to submit a request to the FDA to change the route of administration from subcutaneous to intramuscular and to decrease the six dose priming series from six to five doses.

Question. One of the chief purposes of the Project BioShield Act of 2004 (the "Act") was to provide contracting flexibility to enable the government to more rapidly acquire countermeasures against biological, chemical, radiological or nuclear agents that might be used in terrorist attacks. To what extent has HHS used simplified acquisition procedures in the following Bioshield procurements:

—Solicitation No. DHHS–ORDC–05–01 for Pediatric Formulation of Potassium Iodide;

—Solicitation No. RFP–DHHS–ORDC–04–01 for Licensed Anthrax Recombinant Protective Antigen (rPA) Vaccine for the Strategic National Stockpile;

—Solicitation No. 2004–N–01385 for Therapeutic Products for Treatment of Inhalational Anthrax Disease for the Strategic National Stockpile (the "Anthrax Therapeutics Solicitation"); and

—Solicitation No. 2005–B–01696 for Anthrax Vaccine Adsorbed (BioThrax™).

Answer. Simplified acquisition procedures were not used for these procurements. Some of these products could be obtained only through a sole source, therefore a Justification for Other than Full and Open Competition (JOFOC) was used. Since there was more than one potential source, other products were acquired under full and open competitive procedures as governed by the FAR.

Question. To what extent does HHS plan to use simplified acquisition procedures in the following upcoming procurements:

—Solicitation No. 2004–N–01183 for 200,000 Doses of Heptavalent Botulinum Immune Globulin Reference-Number;

—Request for Information (RFI) ORDC–05–01 for Therapeutics to Treat Neutropenia and Thrombocytopenia Associated with the Acute Radiation Syndrome (ARS); and

—RFI No. ORDC–05–03 for Development and Manufacture of Plasma Derived Human Butyrl-Cholinesterase as a Prophylactice/Therapeutic for Exposure to Nerve Agents?

Answer. For each proposed BioShield procurement, HHS reviews the contract options available and applies the most appropriate authorities to facilitate a fair, technically sound, and rapid acquisition. For example, HHS has selected to use a sole-source acquisition strategy for the procurement of the 200,000 doses of equine heptavalent botulinum immune globulin cited above.

Question. Certain discretionary procurement laws and regulations, such as the requirement for submission of certified cost and pricing data under the Truth in Negotiations Act, place tremendous burdens on commercial entities that do not regularly do business with the Federal Government. Given that the express goal and clear intent of the Act is to encourage greater participation by commercial entities in supplying the Nation with needed countermeasures, to what extent has HHS, in its discretion, required compliance with such laws and regulations (and specifically, the submission of certified cost and pricing data) notwithstanding the existing regulatory exemptions for commercial entities to avoid such unnecessary burdens and the clear intent of the Act to reduce the regulatory burden on procurements conducted under the Act as much as possible?

Answer. In order to obtain the best value to the government and to negotiate a fair price it is essential for the USG to have certified cost and price data unless the contract can be awarded based on adequate price competition. Cost or pricing data is especially needed in regard to those entities that may not as yet have a commercially marketed product or may be using a unique, innovative production process.

Question. Please provide an explanation for any failure in Project Bioshield procurements, both completed or on-going, to use the simplified acquisition authorities granted to HHS under Sections 319F–1(b)(1) and 319F–2(c)(7)(C)(iii) of the Public Health Service Act ("PHSA") as intended by the Act.

Answer. Simplified acquisition procedures have not been used for Project Bioshield procurements to date. Some products could only be obtained through a sole source, therefore a Justification for Other than Full and Open Competition (JOFOC) was used. Since there was more than one potential source, other products were acquired under full and open competitive procedures as governed by the FAR.

Question. Another chief purpose of the Act was to create incentives for manufacturers to develop countermeasures. The main incentive included in the Act was a grant of authority to the Secretary of HHS to issue a call for development of countermeasures and to include in that call a commitment that, upon the first development of a countermeasure that meets the criteria of the Act, the Secretaries of HHS and the Department of Homeland Security ("DHS") will recommend procurement of the countermeasure to the President. This provision was intended to promote the development of a biodefense industry by informing the markets that there is some certainty that there will be a government market for the product. The Act also requires that calls for countermeasures include: an estimated quantity of purchase, necessary measures of minimum safety and effectiveness; estimated price for dose and other information necessary to encourage and facilitate research, development and manufacture of the countermeasure. Sec. 319F–2(c)(4) of the PHSA.

—What calls for countermeasures have been issued by HHS? Please provide copies of these announcements.

—BioShield requires HHS to provide a single estimate of the quantity of countermeasures needed by the government. Has this process been included in every Bioshield procurement to date and if not, why not?

Answer. The publication of a Request for Information (RFI) signals the USG interest in a particular countermeasure. The publication of the Request For Proposal (RFP) is essentially a "call for countermeasures" and indicates, by setting specific requirements and expectations, the government's commitment to an acquisition, including that funds are available to proceed with the procurement. The publication of the RFP and the statement of the specific requirements in the RFP establish that there is a certainty for a government market for the product.

It is expected that most RFPs for BioShield acquisitions will provide a single baseline required quantity for procurement. Some RFPs also may provide options to acquire additional product beyond an initial requirement, based on ongoing threat as-

sessments and ongoing requirements reviews. The RFP for "Therapeutic Products for the Treatment of Inhalation Anthrax Disease" (RFP–2004–N–01385) indicated a range of treatments required (10,000 to 200,000 treatments). This was structured to allow for the flexibility to acquire several products of differing therapeutic classes to meet the stockpile goal.

Question. The Act envisions the use of animal models to permit expedited consideration by the FDA of request for approval for countermeasures. What steps have been taken to assure that the FDA has developed and implemented new procedures under the animal rule and related emergency-like powers under BioShield to signal its commitment to not slow down industries work to develop more countermeasures as quickly as possible?

Answer. The FDA has been actively engaged in the review of animal models and the applicability of the "Animal Efficacy Rule" (Federal Register 67: 37988–37998, 2002) to facilitate the acquisition of critically needed medical countermeasures. Meetings with developers and the review of submissions related to bioterrorism countermeasures are given a priority status. The FDA staff work closely with NIH and DOD staff in the early phases of protocol designs and test methodology development. The FDA has a major role in the Product Development Tools (PDT) Working Group of the Weapons of Mass Destruction Medical Countermeasures Subcommittee which includes representatives of DOD, DHS and USDA as well as HHS. This PDT working group evaluates the need for animals, appropriateness of animal models in use and the need for additional models, facilities and reagents to support medical countermeasures R&D.

Question. As you are aware, the issue of liability protections has been widely discussed as a necessary component to encourage greater participation in Project BioShield. While additional legislation may be needed, what steps has HHS made to maximize use of its existing authorities under Public Law 85–804 and the SAFETY Act to mitigate the risks associated with the development of countermeasures? Specifically, has HHS made clear that indemnification will be included as a contract term during the Request for Proposal process, thus allowing potential bidders the assurance that liability will not be a issue should they be successful in winning the award in advance of incurring proposal costs? If not, why not? Has HHS sought and/or received an exception from the requirement under the implementing Executive Order for Public Law 85–804 that application under the SAFETY Act is a condition for application for indemnification? If not, has HHS been willing to indemnify contractors for risks not otherwise excluded by the SAFETY Act? Has HHS worked with the Department of Homeland Security to integrate the SAFETY Act application process into the procurement process for countermeasures in order to expedite review and consideration of a SAFETY Act application by bidder? If not, why not?

Answer. In a number of instances, HHS has required contractors to apply for SAFETY Act protection as a condition of indemnification. Moreover, we have complied with Executive Order No. 13286, which requires that before granting indemnification, the indemnifying agency obtain (1) the Department of Homeland Security's (DHS) judgment as to whether the agency's requirement may constitute a qualified anti-terrorism technology (QATT) eligible for SAFETY Act protection, and (2) Office of Management and Budget approval in light of the DHS determination.

HHS has not generally indicated in its solicitations that indemnification will be included as a contract term. Subpart 50.4 of the Federal Acquisition Regulation, concerning indemnification under Public Law 85–804, contemplates that contractors will request indemnification, rather than that the procuring agency will offer indemnification on its own initiative. Not all BioShield contractors have sought indemnification. Moreover, the Secretary must personally consider each request for indemnification on its own merits based on contractor submissions regarding, e.g., the availability of insurance. Thus, the contracting officer cannot preempt the Secretary by guaranteeing indemnification in the solicitation.

Executive Order No. 13286 does not require that contractors apply for SAFETY Act protection as a condition of indemnification; rather, as described above, the indemnifying agency must obtain DHS' determination whether the agency's requirement may constitute a QATT eligible for SAFETY Act protection. HHS has not sought an exception to this requirement. HHS has indemnified contractors for risks not excluded by the SAFETY Act.

Question. The Project BioShield Act grants HHS authority to enter into personal service contracts and streamlined personnel authorities to aid in the performance, administration or support of countermeasure research and development. Sec. 319F–1(d) and (e) of the PHSA. To what extent has HHS used this authority? Please explain any failures to use this authority.

Answer. To date, NIAID has used Project BioShield authorities to hire two individuals, with a third appointment pending. The positions filled are:

—One individual in the dual positions of NIAID Associate Director for Biodefense Product Development and Director of the Division of Microbiology and Infectious Diseases' Office of Biodefense Research Activities; salary >$100,000.
—One individual for the position of Associate Director for Product Development in the Division of Allergy, Immunology, and Transplantation; salary >$100,000.
—One individual for the position of Associate Director for Radiation Countermeasures Research and Emergency Preparedness, in the Division of Allergy, Immunology, and Transplantation; salary >$100,000.

Question. Section 5(c) of the Act requires the Secretaries of DHS and HHS to issue a report to Congress within 120 days after the enactment of the Act concerning whether there is a lack of adequate large scale biocontainment facilities necessary for the testing of countermeasures in accordance with Food and Drug Administration requirements. Why has this report not been issued? What work has been done on this report? When will it be issued?

Answer. An interim report was submitted to Congress on April 28 2005, and the final report will be submitted soon. Additional time was needed to sufficiently conduct an assessment of U.S. Biocontainment facilities.

Question. The Act requires the Secretaries of HHS and DHS to enter into an interagency agreement for procurement of countermeasures in accordance with the requirements of the Act. Sec. 319F–2(c)(7)(B). Please provide a copy of this agreement.

Answer. A copy of this agreement as it applies to the acquisition of rPA anthrax vaccine is attached.

Question. The Act requires HHS to institute appropriate controls concerning the use of procurement authorities under the Act. Secs. 319F–1(b)(1)(C) and 319F–2(c)(7)(C)(iii)(III) of the PHSA. Please provide a copy of the written guidance explaining these controls. Does HHS intend to publish the controls as regulations? Does HHS intend to promulgate implementing regulations for the entire Act? If so, when? If not, why not?

Answer. The BioShield Act is sufficiently detailed and prescriptive to obviate the need for regulations. The procurement control process is conducted consistent with the Federal Acquisition Regulations (FAR) and the Health and Human Services Acquisition Regulations (HHSAR). HHS will be happy to provide the Committee with a copy of these documents should you so desire.

QUESTIONS SUBMITTED BY SENATOR ARLEN SPECTER

Question. What role do you envision CDC would play in any new BioShield legislation? Should not CDC be heavily involved in the implementation of any future BioShield program?

Answer. CDC plays a significant role in current BioShield programs. The Strategic National Stockpile (SNS) is located within CDC, is very actively engaged in the BioShield acquisition process, and provides the primary storage sites and distribution mechanisms for BioShield products. Subject matter experts (SMEs) at CDC are participants of the Weapons of Mass Destruction Medical Countermeasure Subcommittee (WMD MC), which reviews and establishes the requirements for BioShield acquisitions.

Section 10 of President Bush's Homeland Security Presidential Directive/HSPD–8 issued in December of 2003 States that "the Secretary of HHS . . . and heads of other Federal departments and agencies that provide assistance for first responders preparedness will base those allocations on assessments of population concentrations, critical infrastructures, and other significant risk factors, particularly terrorism threats, to the extent permitted by law."

Question. Has HHS abided by this Presidential directive in the allocation of State and Local bioterrorism preparedness funding?

Answer. The Department of Health and Human Services (HHS) funding priorities for State and local bioterrorism preparedness are consistent with Homeland Security Presidential Directive 8 (HSPD–8). A large percentage of public health emergency preparedness funds are allocated using a ratio of jurisdictional to U.S. population. In addition, this year CDC allocated funds for mass prophylaxis preparedness in 21 major metropolitan areas through the Cities Readiness Initiative (CRI). Mass preparedness is one of our Nation's priorities as described in the Interim National Preparedness Goal. Urban areas are selected for CRI based on population, risk, threats, and infrastructure. All of the CRI awardees are also Urban Area Security Initiative (UASI) grantees. This year HHS awarded funds to 15 additional metropolitan statistical areas to support preliminary planning for becoming full CRI awardees in fiscal year 2006, as proposed in the President's budget request. CDC

has developed Preparedness Goals designed to measure urgent public health system response performance parameters that are directly linked to health protection of the public. The Preparedness Goals are intended to measure urgent public health system response performance for terrorism and non-terrorism events including infectious disease, environmental and occupational related emergencies. Preparedness measures are a subset of the overarching targeted capabilities list and are consistent with national preparedness goals

Question. What is the process for determining the prioritization of items to be purchased for the Strategic National Stockpile? At what level of the process are the scientists and infectious disease experts of the National Institutes of Health and the Centers for Disease Control and Prevention included?

Answer. The classifications of Category A, B, and C agents (agents that are likely to be used in a bioterror attack) have been generated from infectious disease and medical analyses to which NIH and CDC scientists contributed significantly. We have initially focused our countermeasure procurement efforts on Category A agents that pose the greatest threats. To address the threat of any one particular agent, consideration is given to currently available countermeasures, such as antibiotics and vaccines. Further consideration includes the need for or role of new countermeasures, such as antitoxins, next generation vaccines, or antibiotics. Perceived need and absence of a new countermeasure informs research initiatives. Scientists from OPHEP, NIH, CDC, Food and Drug Administration (FDA), Department of Defense (DOD), and Department of Homeland Security (DHS) are asked to determine which new countermeasures are scientifically advanced enough to invest in advanced development and testing, would have the greatest public health impact, and have the greatest likelihood of success.

The process to determine which countermeasures are placed in the SNS is informed by the interagency WMD MC subcommittee. This is an interdepartmental subcommittee initially chartered by the Office of Science and Technology Policy (OSTP) and co-chaired by senior government officials from DHS, HHS, and DOD. The material threat assessments (MTA) developed by DHS based on a plausible attack scenario informs the sizing of the procurement requirement. HHS, through the coordination efforts of OPHEP, then evaluates the availability of currently developed countermeasures and assesses the scientific opportunities to develop new countermeasures. The WMD MC then deliberates on the nature of the medical consequence and the availability of appropriate countermeasures to develop a recommendation for the acquisition of a specific countermeasure. HHS can issue a Request for Information (RFI) to determine the market availability and to alert industry to the U.S. Government interests. Once a U.S. Government requirement for a particular new medical countermeasure has been established by the WMD MC and approved by OMB is granted, a Request for Proposals (RFP) announcing the specific requirements follows. HHS implements the acquisition process.

QUESTIONS SUBMITTED BY SENATOR ROBERT C. BYRD

LACK OF BIOSHIELD FUNDING FOR RAD/NUC RESPONSE

Question. On April 13th, the Department of Homeland Security wrote Congress notifying us of the creation of the Domestic Nuclear Detection Office. In the letter, the Department justified the creation of the Office based on the assertion that, "The risk that terrorists will acquire and use a nuclear/radiological device is one of the gravest threats that confronts the Nation."

Yet despite this assertion, our Nation is still without a practical way to medically treat the thousands or even hundreds of thousands of Americans who may be exposed or who may believe they have been exposed to radiation in the event we are attacked in this way. While I understand that radiological and nuclear threats have been certified as a "material threat," I was surprised to learn that the Bioshield program has not actually been used to procure several very promising drugs that are now in late-stage development and could be available in the near term to respond to this most insidious of threats.

Beyond your limited plan to purchase pediatric potassium iodide, what is your schedule for procuring drugs for the national stockpile to respond to what is called Acute Radiation Syndrome (ARS)?

Answer. HHS is eager to enlarge the holdings of the SNS with respect to radiological/nuclear countermeasures. A Request for Information (RFI) for countermeasures for an ARS was published in October 2004. Responses have been evaluated; and a Request for Proposals (RFP) is being developed. We anticipate releasing a draft RFP for industry comment on the general topic of ARS as soon as July 2005.

Accordingly, the quality of the proposals and the availability of resources will determine how HHS acts on the results of the RFI and RFP. The SNS currently contains Potassium Iodide, Pediatric Potassium Iodide, Calcium/Zinc Diethylenetriaminepentaacetate (Ca/Zn DTPA) and Prussian Blue (Ferric hexacyanoferrate (II)) as countermeasures for a radiation event. In addition, Granulocyte-Colony Stimulating Factor (G–CSF) is available to the SNS under Investigational New Drug (IND).

PRIVATE SECTOR INTEREST IN BIOSHIELD

Question. When the President signed the BioShield Act into law last July, the Washington Post reported that "Few companies have shown much enthusiasm for diverting staff and money from programs to develop drugs, such as cancer and cholesterol treatments, with bigger and more established markets. Of about 1,000 U.S. biotechnology companies, about 100 are working on biodefense projects, according to the Biotechnology Industry Organization, an industry trade group."

Has the interest in BioShield increased or are companies still reluctant to participate in the program? What recommendations would you make to increase private sector interest in BioShield?

Answer. We have seen significant interest in BioShield, however we recognize the need for continuing improvement and expanded outreach. Many of the innovative approaches to developing a medical countermeasure occur in small biotech companies that are inexperienced in manufacturing, clinical trials, and the regulatory process. They are generally funded by venture capital investors and are operating at a loss. They usually need funds to validate a current Good Manufacturing Practices (cGMP) manufacturing process and to conduct the necessary animal studies or human safety studies to qualify for an Investigational New Drug (IND) application.

The large pharmaceutical companies have numerous opportunities to consider when establishing their business model and the priority targets of their research and development portfolios. They must weigh the opportunity costs for the biodefense market with its intrinsic uncertainty regarding the size and sustainability against more predictable and quantifiable markets for medical products for diseases with relatively well-established target populations, many of which will be sustained over many years. As large pharmaceutical companies consider the profits for traditional medical products versus the profits available for vaccines or other medical countermeasures, the reason for their reluctance appears to be driven by the markets. For example, as mentioned by Dr. Fauci in his February 8, 2005 testimony, a year's supply of Lipitor to lower cholesterol is $1,608; a year's supply of 50-milligram Viagra is $3,500; but a flu vaccine generally sells for $7 to $10.

Today, the U.S. Government is involved throughout the pipeline of countermeasure development, through basic research support at NIH and the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) all the way to the procurement activities undertaken through Project BioShield. Both NIH and the USAMRIID have excellent records in this regard. The U.S. Government can further target and facilitate research and development efforts by setting clear requirements and specifications for: medical countermeasures; facilitating partnerships as needed between government and industry or between industry and industry; and providing critical resources such as facilities (e.g. laboratories with high-level biocontainment), animals (for testing), reagents and assays.

Grant Coordination—for Assistant Secretary Simonson

Question. The recent TOPOFF 3 training event recently portrayed a scenario that exercised first responders, hospital capacity and the ability to treat a sudden rush of people affected by chemical and biological agents. We look forward to a report on the exercise around mid-summer. Since fiscal year 2002, Congress has appropriated $11 billion to first responders through the Department of Homeland Security and $5.5 billion through the Department of Health and Human Services to provide local monitoring for outbreaks and surge capacity for treatment. BioShield has $5.6 billion over 10 years to feed our Strategic National Stockpile. We have committed a significant amount of money into these programs, over $22 billion. However, when tragedy strikes the citizens of this country demand a seamless operation that provides emergency care, timely correct information, and treatment if needed.

Do local health agencies have the capacity and infrastructure to deal with a surge in activity?

Answer. CDC funding, distributed through cooperative agreements, has enabled local health departments to increase both capacity and infrastructure to deal with surges by providing for increased epidemiologic capacity, terrorism preparedness and response trainings for public health practitioners, improved communications systems (in terms of not only equipment but also improved relationships between

the public health, medical and homeland security communities), and enhanced technology and staff in public health laboratories. HHS recognizes that not each of the approximately 4,000 local health departments can or should have the same response capability, especially considering the wide variation in size, risks and populations served as well as a finite amount of funding. Therefore, HHS encourages and supports local health departments to work together to develop regional capacity and infrastructure through shared equipment, personnel, information and other assets. For example, during a mass prophylaxis event, neighboring local health departments might assist the affected jurisdiction in some aspect of the response, such as staffing, so that the local health department can focus on mass prophylaxis.

Local health departments have been developing volunteer pools and strengthening partnerships with other agencies and businesses to provide support activities such as mass prophylaxis. Another example is laboratory capacity—a key asset for public health emergency preparedness and response that is expensive for a local jurisdiction's budget. Not every local health department can have advanced laboratory capability. Therefore, some local health departments have basic laboratory capability and refer some samples to a Laboratory Response Network (LRN) laboratory. Other local health departments have collaborative relationships with neighboring laboratories that have existing capability. The State public health laboratory can provide additional capability to all local health departments within their jurisdiction. While local health departments continue to improve, maintaining this capacity and infrastructure will also be necessary.

For healthcare surge capacity, HHS has proposed in its fiscal year 2006 budget funding for the procurement and maintenance of portable hospital units (Federal Medical Contingency Stations) as a part of its Mass Casualty Intiative. These units can be rapidly deployed to anywhere in the country and would supplement local hospital surge capacity by 5,500 beds in the event of an emergency.

Question. What lessons have we learned through coordinating first responder efforts with medical response efforts?

Answer. *Force Protection.*—Important steps have been taken to establish the necessary medical counter and preventive measures to protect first responders. Vaccination and prophylaxis for the most common agents have been studied and best practices developed. Personal Protective Equipment (PPE) standards have been established by the first responder industry in conjunction with public health. Manufacturers are now certifying equipment such as Self Contained Breathing Apparatus (SCBA) as Weapons of Mass Destruction (WMD) compliant.

Surge.—Issues of surge capacity have been addressed in multiple ways. Solutions are being sought both in and out of the hospital. Within the hospitals, mechanisms are being implemented to open beds in case of a catastrophic incident. These mechanisms include the use of adding beds to the existing infrastructure as well as discharging or transferring patients who could receive care elsewhere. First responders are being asked to support efforts to sustain develop and various levels of treatment outside the hospitals that are free standing or potentially an annex to an existing hospital.

Incident Command Structure.—With the advent of the National Incident Management System (NIMS) and the National Response Plan (NRP), we now have a common methodology for managing an event that incorporates first responders and medical communities. As planning efforts continue to move forward in these communities, the essential link between them may be articulated.

Forensic Epidemiology.—CDC has created a course on Forensic Epidemiology in collaboration with the Federal Bureau of Investigation (FBI) from which more than 13,000 public health and law enforcement officials have graduated. Criminal and epidemiological investigative methods are used to demonstrate an understanding of the similarities and differences in public health and law enforcement investigative goals and methods. Common operating procedures about how finding are communicated between the two groups are of primary importance.

Equipment Standardization.—HHS has supported the efforts and participated in the Interagency Board (IAB) for Equipment Standardization and Inter Operability Working Group since its inception. The IAB is designed to "establish and coordinate local, State, and Federal standardization, interoperability, and responder safety to prepare for, respond to, mitigate, and recover from any incident by identifying requirements for Chemical, Biological, and radiological, Nuclear or Explosives incident response equipment."

Early Event Detection (Syndromic Surveillance).—Information recorded by the first responders such as 9–1–1 call information, Emergency Medical Services patient care records, and other public health data are reviewed for statistical anomalies in the syndromes that present. These anomalies are reviewed against signs and symptoms of bio and chemical terrorism, as well as unforeseen natural disease outbreaks.

By collaborating with the first responder community, public health authorities can obtain advanced insight into the changing health conditions of a given population or frequency with which they occur.

Decontamination.—The capability of first responders to properly decontaminate hundreds of people has become well established in the majority of metropolitan statistical areas, which can be attributed in large part to leadership from Health Resources and Services Administration (HRSA) grants. Hospitals understand the importance of not allowing facilities to become contaminated, and have taken important steps to protect themselves. While acute mass decontamination continues to be a challenge, significant efforts are under way to develop methods to quickly decontaminate thousands of people.

Rapid Registry.—The Rapid Response Registry (RRR) is an HHS response tool intended to assist local officials in rapidly identifying, enumerating, and obtaining contact information for individuals who have been, or who believe they may have been, exposed. The emergency contact information collected is necessary for both short-term and long-term follow-up for exposed, injured, and ill individuals and would be available to public health officials to guide public health response services directed at the affected population during the emergency response. In addition to the data collection tool, the Agency for Toxic Substances and Disease Registry (ATSDR) staff can provide either remote or on-scene technical assistance to support public health needs assessment activities, medical assistance, health interventions, or health education in the affected population during or immediately following the recognition of a Chemical, Biological, Radiological, and Nuclear Warfare, and Explosives (CBRNE) emergency. This process allows State and local public health responders to target enrolled individuals with updated information, triage their specific risk for potential exposures, determine appropriate self-decontamination procedures, and recommend any immediate medical evaluation or interventions (countermeasures). Real time data collection also enables future health studies by State and local public health as part of long-term mitigation activities, should these be determined appropriate.

HHS Secretary's Emergency Response Team (SERT).—The SERT acts as the Secretary's agent on emergency sites working along with the first responder community under the direction of the Assistant Secretary for Public Health Emergency Preparedness (ASPHEP). The ASPHEP, on behalf of the Secretary, directs and coordinates the Department's efforts to prevent, prepare for, respond to, and recover from, the public health and medical consequences of disaster or emergency. The SERT directs and coordinates the activities of all HHS personnel deployed to the emergency site to assist State, local, Tribal, and other Federal and government agencies as applicable.

Health Alert Network (HAN).—The HAN ensures that each community has rapid and timely access to emergent health information; a cadre of highly-trained professionals; and evidence-based practices and procedures for effective public health preparedness, response, and service on a 24/7 basis. The HAN is dedicated to strengthening the core public health infrastructure for information access, communications, and distance learning at the State and community levels. Through continuous, high-speed internet connectivity and broadcast capacity to support emergency communication, HAN provides the national public health system with a network of public health officials and other first-responders who are continuously connected to information vital to emergency and non-emergency public health practice.

Medical Reserve Corp (MRC).—MRC units are community-based and function as a way to locally organize and utilize volunteers who want to donate their time and expertise to prepare for and respond to emergencies, and promote healthy living throughout the year. MRC volunteers supplement existing first responders and public health resources. MRC volunteers include medical and public health professionals such as physicians, nurses, pharmacists, dentists, veterinarians, and epidemiologists. Many community members—interpreters, chaplains, office workers, legal advisors, and others—also fill key support positions in the first responder community.

SNS.—The SNS has large quantities of medicine and medical supplies to protect the American public if there is a public health emergency severe enough to drain local supplies. Should Federal and local authorities agree that the SNS is needed, medicines will be delivered to any State in the United States or territory within 12 hours. Each of our 62 grantees has plans to receive and distribute SNS medicine and medical supplies to local communities as quickly as possible. Many of these medical countermeasures will initially be used by the first responder community so that they can continue to fulfill their vital role in support of an event.

The National Incident Communications Coordination Line (NICCL).—NICCL is a special toll free line with limited access via PIN number, is maintained by DHS and

is used to bring together the key Public Affairs representatives from Federal, State and local agencies during major incidents. DHS convenes calls to ensure all agencies are fully aware of the facts concerning the incident, achieve agreement as to which agencies have the public communications lead concerning the various aspects of the incident and coordinate all public announcements concerning the incident. The NICCL has been used effectively during a number of incidents over the past year and as part of the Top Officials 3 (TOPOFF3) exercise. In each case not only Federal agencies participated in the calls but also State and local Public Affairs Officers from the affected areas were included.

Question. Are grant programs coordinated by DHS and HHS so that Americans, in their time of need, are protected and treated to the highest standard possible without confusion or lack of direction?

Answer. HHS cooperative agreement programs and DHS grant programs are being coordinated at the Federal, State, and local levels. Since 2003 HHS has required that the State-wide joint advisory committees required by CDC and HRSA cooperative agreements include members from State homeland security or emergency management, fire, and police agencies. In 2005, DHS added similar language to its program guidance documents, which now requires State homeland security agencies to reach out to the public health and medical communities. Many intrastate coordinating bodies, which have been established by local jurisdictions, require participation by homeland security, emergency management, public health, and medical communities in regional planning and response efforts as well. HHS also requires its awardees to comply with the NIMS, which facilitates coordination, communication and cooperation between first responders (e.g., fire, police, public health) and first receivers (e.g., hospitals) during an event.

At the Federal level, both HHS and DHS review and comment on the program announcements and guidance documents of their sister agencies, to which States and local jurisdictions respond in order to receive funds. Both Departments also have ten regional emergency coordinators, who work closely with one another and with States to plan, train and exercise across jurisdictional lines. More recently, HHS and DHS have formed a steering committee to identify additional mechanisms to increase coordination and collaboration between the awardees and grantees, as well as between the Departments at the Federal level. Future activities may include joint site visits and regional meetings.

BioShield Benchmarks—for Assistant Secretary Simonson

Question. In 1999, Congress charged the Department of Health and Human Services and the Centers for Disease Control and Prevention with the establishment of the National Pharmaceutical Stockpile. The Homeland Security Act of 2002 renamed the effort the Strategic National Stockpile and tasked the Department of Homeland Security with defining the goals and performance requirements but the Stockpile was to be jointly managed by DHS and HHS. The Project BioShield Act of 2003 returned oversight and guidance of the stockpile to HHS.

With all of the changes in command, what information and tools are we using to ensure that Project BioShield is properly feeding the Strategic National Stockpile so that it is truly ready to provide rapid access to large quantities of the right types of pharmaceuticals and medical supplies? What specific benchmark are we using to gauge ourselves in the ability to respond to an unknown attack or natural disaster?

Answer. The SNS staff has remained intact during the recent departmental changes. In addition, the deliberative process to set requirements and implement acquisitions for the SNS under Project BioShield has also remained constant. The SNS engages in deployment exercises with various State and local entities on a regular schedule to assess the readiness of State and local partners and to improve the deployment process. In addition, CDC and the SNS participate in National and international exercises, such as TOPOFF3, to fully assess their response capabilities for communication, logistics, resource allocations, and stockpile utilization. These exercises serve as a benchmark for the Nation's level of preparedness for an unknown or natural disaster. SNS performance measures to deliver assets within 12 hours of decision to deploy. While project Bioshield is focused on development of new countermeasures which will be incorporated into SNS once available, SNS acquires and maintains significant countermeasures currently available.

CONCLUSION OF HEARINGS

Senator GREGG. Well, if you have got thoughts, we would be interested in language you think would improve that because I do be-

lieve unless we address this issue of liability, we will never get this straightened out and we will never get the participation we need.

Well, all of your input has been excellent. I am trying to think of what title we should have on this novel award. We will have to come up with something. We will call it the Franz award.

In any event, thank you very much. We appreciate your input. This is not an end. This is just an ongoing discussion as to how we make this whole system work better and just one part of the discussion. We intend to continue to pursue this as a committee. You obviously intend to pursue it as professionals. So thank you.

Dr. READ. Thanks for your leadership.

Senator GREGG. The subcommittee is recessed.

[Whereupon, at 12:15 p.m., Thursday, April 28, the hearings were concluded, and the subcommittee was recessed, to reconvene subject to the call of the Chair.]

DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR FISCAL YEAR 2006

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

NONDEPARTMENTAL WITNESSES

[The following testimonies were received by the Subcommittee on Homeland Security for inclusion in the record. The submitted materials relate to the fiscal year 2006 budget request for programs within the subcommittee's jurisdiction.]

PREPARED STATEMENT OF THE AMERICAN PUBLIC TRANSPORTATION ASSOCIATION

Mr. Chairman, thank you for this opportunity to submit written testimony on the security and safety of public transportation systems. We appreciate your interest in transportation security, and we look forward to working with you as you develop the fiscal year 2006 appropriations bill for the Department of Homeland Security (DHS).

ABOUT APTA

The American Public Transportation Association (APTA) is a nonprofit international association of over 1,500 public and private member organizations including transit systems and commuter rail operators; planning, design, construction, and finance firms; product and service providers; academic institutions; transit associations and State departments of transportation. APTA members serve the public interest by providing safe, efficient, and economical transit services and products. Over 90 percent of persons using public transportation in the United States and Canada are served by APTA member systems.

OVERVIEW

Mr. Chairman, public transportation is one of our Nation's critical infrastructures. We cannot over-emphasize the critical importance of our industry to the economic quality of life of this country. Over 9.6 billion transit trips are taken annually on all modes of transit service. People use public transportation vehicles over 32 million times each weekday. This is more than 16 times the number of daily travelers aboard the Nation's airlines.

Safety and security are the top priority of the public transportation industry. Transit systems took many steps to improve security prior to 9/11 and have significantly increased efforts since then. Since September 11, 2001, public transit agencies in the United States have spent over $2 billion on security and emergency preparedness programs and technology, almost all from their own budgets with only minimal Federal funding. Last year's events in Madrid further highlight the need to enhance security on public transit systems and to do so without delay. We do not need another wakeup call like Madrid.

In response to an APTA survey, transit agencies around the country have identified in excess of $6 billion in transit security needs. State and local governments and transit agencies are doing what they can to improve security, but it is important that the Federal Government be a full partner in the effort to ensure the security of the Nation's transit users.

In fiscal year 2003, transit security received $65 million in Federal funding from DHS. In fiscal year 2004, $50 million was provided for Federal transit security programs from DHS. For the first time in fiscal year 2005, Congress specifically appro-

priated $150 million for transit, passenger and freight rail security. Out of the $150 million, transit will receive approximately $130 million—almost $108 million for rail transit and more than $22 million for bus. Also, ferries will receive an additional $5 million for security from a separate account. We are very appreciative of this effort. However, in the face of significant needs, more needs to be done.

We urge Congress to act decisively on this issue. In light of the documented needs, we respectfully urge Congress to provide $2 billion in the fiscal year 2006 Homeland Security Appropriations bill for transit security. Of that amount, we recommend that $1.2 billion be provided for capital needs, and $800 million for transit costs. Federal funding for needs should provide for, among other things, planning, public awareness, training and additional transit police.

We are disappointed that the Administration recommended only $600 million for a Targeted Infrastructure Protection Program in the fiscal year 2006 DHS budget proposal, which would fund infrastructure security grants for transit, seaports, railways and energy facilities. We were also disappointed that the Administration does not include a specific line item funding amount for transit security. We look forward to working with the Administration and Congress in securing adequate transit security funding that begins to address unmet transit security needs of the country.

We further request that the existing process for distributing DHS Federal grant funding be modified so that funds are distributed directly to transit authorities, rather than to State Administrating Agencies (SAA). While we are willing to coordinate with the States and urban areas that we serve, we believe direct funding to the transit authorities would be more efficient and productive.

We are pleased to note that APTA has become a "Standards Development Organization" (SDO) for the public transportation industry. Our efforts in standards development for commuter rail, rail transit and bus transit operations over recent years have been significant and our status as a SDO has been acknowledged by both the Federal Transit Administration (FTA) and the Federal Railway Administration (FRA). The FTA and the Transportation Research Board have also supported our standards initiatives through the provision of grants. We would like to apply our growing expertise in standards development of transit industry safety and security, best practices, guidelines and standards. We look forward to working with the Administration and Congress in support of this initiative and trust that Federal financial assistance would be made available to develop such standards and practices.

We also would like to work with Congress and the Department of Homeland Security's Directorate of Science and Technology to take a leadership role in advancing research and technology development to enhance security and emergency preparedness for public transportation.

SECURITY INVESTMENT NEEDS

Mr. Chairman, after the awful events of 9/11, the transit industry invested some $2 billion in enhanced security measures, building on the industry's already considerable efforts. At the same time, our industry undertook a comprehensive review to determine how we could build upon our existing industry security practices. This included a range of activities, some I discussed earlier in testimony, which include research, best practices, education, information sharing in the industry, and surveys. As a result of these efforts we have a better understanding of how to create a more secure environment for our riders, and the most critical security investment needs.

Our latest survey of public transportation security identified enhancements of at least $5.2 billion in additional capital funding to maintain, modernize, and expand transit system security functions to meet increased security demands. Over $800 million in increased costs for security personnel, training, technical support, and research and development have been identified, bringing total additional transit security funding needs to more than $6 billion.

Responding transit agencies were asked to prioritize the uses for which they required additional Federal investment for security improvements. Priority examples of operational improvements include:

—Funding current and additional transit agency and local law enforcement personnel.
—Funding for over-time costs and extra security personnel during heightened alert levels.
—Training for security personnel.
—Joint transit/law enforcement training.
—Security planning activities.
—Security training for other transit personnel.

Priority examples of security capital investment improvements include:

—Radio communications systems.
—Security cameras on-board transit vehicles and in transit stations.
—Controlling access to transit facilities and secure areas.
—Automated vehicle locator systems.
—Security fencing around facilities.

Transit agencies with large rail operations also reported a priority need for Federal capital funding for intrusion detection devices.

Mr. Chairman, the Department of Homeland Security issued directives for the transit industry in May 2004, which would require that transit authorities beef up security and to take a series of precautions which would set the stage for more extensive measures without any Federal funding assistance. We believe these directives are unfunded mandates. Many of our transit systems have already carried out most of the measures that Transportation Security Administration (TSA) is calling for, such as drafting security plans, removing trash bins and setting up procedures to deal with suspicious packages. The cost of these measures and further diligence taken during times of heightened alert is of particular concern to us. We look forward to working with you in addressing these issues.

As you know, in the fiscal year 2005 Homeland Security Appropriations bill (Public Law 108–334), TSA can hire up to 100 rail inspectors using a $10 million appropriation. We have concerns about this provision. We believe that funding for the inspectors would be better spent on things that would support the industry such as surveillance cameras, and emergency communication and other systems rather than highlighting security issues without providing the necessary resources to address them. We look forward to working with you in addressing our concerns.

BACKGROUND

Mr. Chairman, prior to and following September 11, 2001—the date of the most devastating terrorist attack in U.S. history—APTA has played a key role in addressing the safety and security issues of our country. American public transportation agencies have also taken significant measures to enhance their security and emergency preparedness efforts to adjust to society's new state of concern. Although agencies had a wide range of security initiatives in place at the time of the World Trade Center and Pentagon attacks and already had developed emergency response plans, the September 11 incidents focused, strengthened and prioritized security efforts throughout the industry.

Transit agencies have had an excellent safety record and have worked for years to enhance their system security and employee security training, by following government standards and APTA guidelines, and by learning from the attacks on transit agencies abroad. For example, the 1995 sarin gas attack in the Tokyo subway system caused U.S. transit properties managing tunnels and underground transit stations to go on high alert. The San Francisco Bay Area Rapid Transit District, for instance, responded to the potential threat of chemical weapons attacks by sending a transit police team to Fort McClellan, Alabama, to learn response tactics from U.S. Army chemical weapons experts.

In the months following the September 11 terrorist attacks, transit agencies of all sizes worked to identify where they might be vulnerable to attacks and increased their security spending for both operations and capital costs. The agencies subsequently upgraded and strengthened their emergency response and security plans and procedures, taking steps to protect transit infrastructure and patrons and to increase the transit security presence while giving riders a sense of security.

Some initiatives around the country include:
—Increased surveillance via closed circuit TV;
—Increased training for employees;
—Hired more police, K–9 units added;
—Chemical detection systems being tested;
—Infrastructure design to eliminate hiding places;
—Drills are routinely held with first responders; and
—Encouraging riders to be vigilant for suspicious activities or items.

After September 11, transit systems enhanced efforts to prevent unauthorized entry into transit facilities. The need for employees and passengers to stay alert and report suspicious occurrences became a key goal of many agencies. These efforts are paying off. But, while many transit agencies are more secure than they were prior to September 11, more can and should be done.

APTA has launched additional efforts to further transit industry security and preparedness, collaborating with FTA in developing emergency preparedness forums, and sponsoring and organizing security-related conferences and workshops. Moreover, APTA developed a list of critical safety and security needs faced by the transit

industry, which it has provided to the Department of Transportation and the U.S. Congress.

PUBLIC TRANSPORTATION INFORMATION SHARING ANALYSIS CENTER (ISAC)—NEED FOR ONGOING FUNDING

Presidential Decision Directive Number 63 authorizes and encourages national critical infrastructures to develop and maintain ISACs as a means of strengthening security and protection against cyber and operations attacks. APTA is pleased to have been designated a public transportation Sector Coordinator by the U.S. Department of Transportation, and in that capacity has received a $1.2 million grant from the Federal Transit Administration to establish a transit ISAC. APTA formalized an agreement with a private company to implement the ISAC and make it available to public transit systems around the country.

This ISAC for public transit provides a secure two-way reporting and analysis structure for the transmission of critical alerts and advisories as well as the collection, analysis and dissemination of security information from transit agencies. The public transit ISAC also provides a critical linkage between the transit industry, the U.S. Department of Transportation, the Transportation Security Administration, and the Department of Homeland Security.

The Public Transit ISAC has been invaluable to the public transit industry. However, its 2-year funding from the FTA has expired, and even though APTA pursued future funding for the ISAC from DHS and other agencies, we were not successful. DHS has decided it will no longer provide funding for ISACs. Instead, DHS has launched a new program—Homeland Security Information Network-Critical Infrastructure (HSIN–CI), in which we are participating. HSIN is designed to provide a new set of tools to share critical sector information among private industry and government, but a fully functioning HSIN has yet to be realized. Once it is, there is no guarantee that it will ever be as useful and comprehensive as the Public Transit ISAC. Consequently, we believe that ongoing, reliable and consistent funding from Congress for the Public Transit ISAC is necessary.

ONGOING TRANSIT SECURITY PROGRAMS

Mr. Chairman, while transit agencies have moved to a heightened level of security alertness, the leadership of APTA has been actively working with its strategic partners to develop a practical plan to address our industry's security and emergency preparedness needs. Shortly after the September 11 events, the APTA Executive Committee established a Security Task Force. The APTA Security Task Force has established a security strategic plan that prioritizes direction for our initiatives. Among those initiatives, the Task Force serves as the steering group for determining security projects with more than $2 million in Transit Cooperative Research funding through the Transportation Research Board.

Through this funding, APTA has conducted four transit security workshop forums around the Nation for the larger transit systems with potentially greater risk exposure. These workshops provided confidential settings to enable sharing of security practices and applying methodologies to various scenarios. The outcomes from these workshops were made available in a controlled and confidential format to other transit agencies unable to attend the workshops. The workshops were held in New York, San Francisco, Atlanta, and Chicago.

In partnerships with the Transportation Research Board, the APTA Security Task Force has also established two TCRP Panels that identified and initiated specific projects developed to address Preparedness/Detection/Response to Incidents and Prevention and Mitigation. The Security Task Force emphasized the importance for the research projects to be operationally practical.

In addition to the TCRP funded efforts, a generic Checklist For Transit Agency Review Of Emergency Response Planning And System Review has been developed by APTA as a resource tool and is available on the APTA web site. Also through the direction of the Security Task Force, APTA has reached out to other organizations and international transportation associations to formally engage in sharing information on our respective security programs and to continue efforts that raise the bar for safety and security effectiveness.

APTA has long-established Safety Audit Programs for Commuter Rail, Bus, and Rail Transit Operations. Within the scope of these programs are specific elements pertaining to Emergency Response Planning and Training as well as Security Planning. In keeping with our industry's increased emphasis on these areas, the APTA Safety Audit Programs have been modified to place added attention to these critical elements.

CONCLUSION

Mr. Chairman, in light of our Nation's heightened security needs post 9/11, we believe that increased Federal investment in public transportation security by Congress and DHS is critical. The public transportation industry has made great strides in transit security improvements since 9/11 but much more needs to be done. We look forward to building on our cooperative working relationship with the Department of Homeland Security and Congress to begin to address these needs. We again thank you and the Committee for allowing us to submit testimony on these critical issues, and look forward to working with you on safety and security issues.

PREPARED STATEMENT OF THE ASSOCIATION OF STATE FLOODPLAIN MANAGERS, INC.

The Association of State Floodplain Managers, Inc. (ASFPM) is pleased to share comments on these key aspects of the fiscal year 2006 budget proposal for FEMA, which we believe greatly impact the ability to reduce the Nation's risk and cost from flooding (or natural hazards):

—Urge transfer of funds from the National Flood Insurance Fund to the Flood Mitigation Fund in the amounts authorized in 2004 to deal with the drain represented by repetitively flooded, insured properties.
—Support for continued full funding for modernization of flood maps, with comments about quality and the need to re-evaluate the funding and duration of the effort.
—Restore the 15 percent formula for the Hazard Mitigation Grant Program funding in States with Basic Mitigation Plans and oppose the Administration's proposed reduction of Hazard Mitigation Grant Program funds from 20 percent to 12.5 percent for States that have Enhanced Mitigation Plans approved by FEMA.
—Monitor how the Department of Homeland Security addresses natural hazards, which each year threaten nearly every local jurisdiction to some degree, and how the Department addresses mitigation programs intended to bring about long-term reduction in the impacts of hazards.
—Clarify that mitigation funds provided to private property owners under FEMA's programs are not taxable as income.

The Association of State Floodplain Managers, Inc., and its 20 State chapters represent over 7,000 State, local, and private sector officials as well as other professionals who are engaged in all aspects of floodplain management and hazard mitigation. All are concerned with reducing our Nation's flood-related losses and reducing the costs of flooding.

Transfer Funds to Address the NFIP'S Repetitive Loss Problem

Following several years of deliberation, Congress enacted the Flood Insurance Reform Act of 2004. In large part, the Act is intended to provide FEMA, States and communities with the funding and tools needed to deal with the National Flood Insurance Program (NFIP) repetitive loss problem. For many years FEMA has identified the disproportionate amount of repetitive claims paid on a very small percentage of NFIP-insured properties as the most significant factor that drives increases in the cost of flood insurance—which affects 4.4 million policyholders in every State and over 20,000 counties, cities and towns. Fewer than 50,000 properties account for a drain of approximately $200 million a year.

The Reform Act of 2004 authorizes transfers of funds (total of $90 million) from the National Flood Insurance Fund (which contains only premium and fee income, no General Funds) into the National Flood Mitigation Fund to aggressively mitigate repetitive loss structures. Funds authorized for three elements of the Flood Mitigation Assistance program are: Basic ($40 million/year), Pilot ($40 million/year through fiscal year 2009), and Individual Property ($10 million/year). The Basic Program is mature, with virtually all States currently active to some degree. For the fiscal year 2006 Basic Program the Administration requests $28 million, just $8 million over the funding level of recent years. No funds were requested for the Pilot Program and the Individual Property Program.

FEMA consistently asserts the merits of focusing mitigation efforts on repetitive loss properties in order to help stabilize and strengthen the National Flood Insurance Fund (NFIF). The Reform Act of 2004 directs that the repetitive loss programs be funded by transfer from the NFIF without differentiating between fee income and premium income. DHS Undersecretary Mike Brown testified that the budget request is limited to only the additional $8 million for the Basic FMA program because the Department is studying how to fund the repetitive loss effort from fee income. ASFPM believes it is appropriate to transfer funds, without further delay,

from fee income and/or premium income. Since the NFIF as a whole will benefit—and all policyholders will benefit if the pressure to raise the rates is diminished—then it is well worth the investment of some premium income.

—ASFPM urges the Subcommittee to fully fund the Flood Mitigation Assistance programs authorized in the Flood Insurance Reform Act of 2004 by transferring funds from the National Flood Insurance Fund to the National Flood Mitigation Fund.

—ASFPM urges the Subcommittee to make clear that transfer funds for the repetitive loss grant programs may be taken from premium income and/or fee income, subject to the limitations of the Reform Act of 2004.

Continue Support for Flood Map Modernization

Flood maps are used for many purposes beyond the immediate needs of the National Flood Insurance Program. Good flood maps play a major role in disaster cost reduction—they are used to support land use and management of identified flood-prone areas. FEMA estimates that local regulation of flood hazard areas, using the flood maps, avoids property losses of over $1 billion each year. FEMA's estimate does not count the benefits associated with using the maps to guide development to less hazard-prone areas. Quality flood maps yield benefits at all levels of government. They help reduce the need for Federal disaster assistance and casualty loss tax deductions because at-risk homes with federally-backed mortgages are required to be covered by flood insurance, which provides financial resources to help owners recover.

ASFPM is concerned that rigid metrics imposed on FEMA are driving map production, rather than the goal of producing defensible and accurate flood maps that reflect necessary revisions. Further, budget constraints created by an out-of-date estimate of map needs is artificially restricting restudies and new studies to only a small number of streams or short reaches of coastline. The expectation that revised flood maps will meet high quality standards is an incentive and justification for States and communities to invest their own funds in the modernization effort—ASFPM is concerned that this expectation is not being met.

—ASFPM strongly endorses the Administration's request for $200 million.

—ASFPM urges the Subcommittee to request that FEMA re-evaluate the duration and anticipated funding levels required to produce revised and updated flood risk maps to the appropriate and defensible quality standards. Re-evaluation is warranted because of advances in technology, lessons learned in the early years of this effort, improved understanding of the extent of areas not adequately mapped, priorities identified by States and communities, and the number of partnership efforts with States and communities, including in-kind and other contribution.

—ASFPM urges the Subcommittee to express its expectation that FEMA will address State-identified priorities and that adequate quality data and mapping for streams and coastlines where people are at-risk are the objectives.

Restore 15 percent Formula for Hazard Mitigation Grant Program and Reject Reduction of Funding Available for States with Enhanced Mitigation Plans

ASFPM urges restoration of the 15 percent formula used to determine amounts made available after disasters for the Hazard Mitigation Grant Program (HMGP) authorized by Section 404 of the Stafford Act. States and communities across the country have evidence that the most effective time to garner support for mitigation projects is in the aftermath of disasters. While mitigation planning is a vital activity to identify hazards and potential risks, only actual damaging events generate significant public interest and State and local financial support. Redundant Regardless of the statistical evidence of the likelihood of future disaster occurrence, communities rarely place hazard mitigation above today's demands for education, social programs, local first responders, and the like. This is especially true in smaller communities where financial resources are always tight.

On the proverbial sunny day,' flooding is a low priority for the millions of homeowners and business owners in the Nation's flood hazard areas—regardless of the mounting evidence that future floods will occur. Homeowners and business owners view offers for buyouts, elevations, and retrofit floodproofing very differently when they are shoveling mud, coping with toxic mold, or faced with collapsed foundations. Restoring HMGP to the 15 percent formula will provide resources to those who have just experienced damage and are most receptive to change.

ASFPM recommends that pre-disaster funding be directed to community-based planning in order to prepare communities to undertake mitigation projects when the disaster strikes. It would also be reasonable to make pre-disaster mitigation funds available to support public projects that address at-risk State and community build-

ings, facilities, and public infrastructure—among the more costly categories of post-disaster public assistance. These projects, which do not require direct and voluntary participation of property owners, can readily be designed and implemented in the pre-disaster context and provide broad public benefits.

—ASFPM urges the Subcommittee to restore the Hazard Mitigation Grant Program formula to 15 percent of certain Federal disaster expenditures. The Disaster Mitigation Assistance Act of 2000 calls for communities to have pre-disaster local mitigation plans in order to access HMGP. One result of this requirement is that communities will be better prepared to identify eligible activities after the next declared disaster, thus further shortening the time needed to obligate and expend the HMGP funds.

—ASFPM urges the Subcommittee to reject the Administration's proposed reduction in the formula to determine amounts available to States with Enhanced Mitigation Plans. To qualify for HMGP based on the 20 percent that is authorized by the Stafford Act, a State demonstrates a strong commitment by administering a comprehensive mitigation program, including having the capability and capacity to manage grants and assess the cost avoidance of mitigation measures. The potential availability of the increased HMGP amount is a powerful incentive for States to take on the significant additional responsibility to work with communities and others to identify and implement feasible and cost-effective mitigation measures.

—ASFPM recommends that the Subcommittee examine the effectiveness of the nationwide, competitive Pre-Disaster Mitigation program. In the fiscal year 2005 appropriations bill DHS was directed to consult with State mitigation officials. Last fall State officials were provided just 2 weeks to respond and, to date, no report has been released. ASFPM recommends that particular attention should be paid to citizen, community and State interest in pre-disaster mitigation and how the ability to provide the non-Federal cost share differs in the pre- and post-disaster periods.

Monitor How the Department of Homeland Security Addresses Natural Hazards and Mitigation

Floods, hurricanes, severe storms, tornadoes, harsh winter storms, landslides, wildfires, and earthquakes put millions of Americans are at risk every day. From a cost and future consequences perspective, ASFPM remains concerned with the diminished focus on natural hazards and mitigation by the Department of Homeland Security. Despite continued assertions of commitment to FEMA's all-hazards mission, DHS has reduced cohesiveness of programs and reduced the number of staff who deal with natural hazards and mitigation. The following remain specific concerns: transferring FEMA funds to areas of DHS that are not under the jurisdiction of the Under Secretary for Emergency Preparedness & Response; detailing FEMA staff out of that directorate; and reducing support for the vital network of State and local public safety and disaster mitigation officials.

DHS Secretary Chertoff is beginning a thorough examination of threats and vulnerabilities in order to prioritize them, and has expressed his intent to align DHS resources and priorities based on this analysis. Natural hazards are a threat in every State—every State has experienced multiple devastating floods that resulted in declaration of major disasters. Damage due to floods of all magnitudes are estimated as exceeding $5 billion each year. Most areas are at risk to other natural hazards, as well. Clearly, our communities and our citizens are vulnerable. ASFPM hopes that adequate consideration of natural hazards is made in the analysis called for by Secretary Chertoff.

—ASFPM urges the Subcommittee to monitor DHS proposals and actions that affect FEMA programs and staff to prevent unwise and unnecessary reduction in FEMA's effectiveness, which in turn will jeopardize State and local efforts to deal with natural hazards and mitigation.

Clarify that Mitigation Grant Funds Received by Private Property Owners are not Taxable as Income

In 2004 the IRS made a determination that mitigation grants to property owners who work with their communities and States to prevent and minimize future damages to their homes and businesses are taxable as income. This decision is having a dramatic impact on the Nation's ability to reduce future damages and costs (many disaster costs are paid directly by taxpayers). Property owners, when told that mitigation cost-share grants will be taxable, are simply opting to NOT mitigate, thus remaining at-risk to future damage. Ironically, property owners are only eligible for cost sharing mitigation grants if it is clearly shown that the benefits to the Nation outweigh the costs to the Nation.

—ASFPM urges the Subcommittee to include language in the appropriations bill to clarify that mitigation cost sharing grants are not taxable income.

For information about ASFPM and this testimony, contact Larry Larson, Executive Director, at (608) 274–0123 (asfpm@floods.org) or Rebecca Quinn, Legislative Officer, at (410) 267–6968 (rcquinn@earthlink.net).

PREPARED STATEMENT OF THE CITY OF SAN MARCOS, TEXAS

Mr. Chairman and Members of the Subcommittee: On behalf of the City of San Marcos, Texas, I am pleased to submit this statement in support of our request for project funding through the Appropriations Bill for Homeland Security.

The City of San Marcos requests an appropriation of $5,000,000 for the San Marcos Municipal Airport to construct and equip a multi-purpose fire station and fire fighter training facility. We would respectfully suggest that this project would properly fall within the scope of first responder, emergency preparedness and response training. There is no provision for this funding in the President's budget, nor has there been any prior year Federal funding.

The City of San Marcos and facility users would be actively engaged in the project's funding through cost-sharing. Approximately $200,000 would be provided by the City for all required real estate and utilities. The City and facility users would provide an estimated $600,000 annually in operating revenues when the facility is fully functional.

The San Marcos Municipal Airport is a public general aviation airport owned and operated by the City of San Marcos, Texas. It is located just east of Interstate Highway 35 on Texas Highway 21 approximately 30 miles south of Austin and 45 miles north of San Antonio. The airport occupies the site of a closed military air base, and we share the former military base with the Department of Labor's Gary Job Corps Center.

There are currently 225 aircraft based at the airport, and the airport supports over 100,000 air operations annually. This makes the San Marcos Municipal Airport the largest and most active general aviation airport in the bustling Austin-San Antonio corridor. To serve the present and future safety and security needs of the airport, an emergency response capability, known in aviation terms as an Aircraft Rescue and Fire Fighting (ARFF) facility, has been among our highest priority goals. We have encountered a challenge in obtaining Federal funding assistance through conventional Federal Aviation Administration channels. In order for the airport to qualify for ARFF funding, the airport must first be certified under Federal Air Regulation, Part 139; however, to achieve certification, the airport requires an ARFF.

As a better, more cost-efficient approach to achieving our goal, we are proposing to partner with the San Marcos Fire Department and the Gary Job Corps Center to construct and equip a facility on the airport that will meet the airport ARFF requirement, serve as a fire station for the City of San Marcos, and also be a training venue for the Gary Job Corps Center and other regional agencies to train fire fighters and emergency service first responders.

Our plan proposes to construct, equip, and then operate a multi-purpose fire station and fire fighter training facility located on the airport. The fire station would consist of two components. One would be a Federal Aviation Administration certified ARFF to meet the evolving public safety and security requirements of a growing public airport. Another component would be a conventional City of San Marcos fire station to be integrated with the San Marcos Fire Department's other emergency response forces to serve the citizens of San Marcos.

In addition to these two emergency response capabilities, the facility would be the educational site and provide support to the Gary Job Corps Center's mission of training students for careers as professional fire fighters and emergency service first responders. We further envision that the facility will serve other regional training needs, especially for the many small community and rural emergency services responders who do not have the resources to maintain their own training facilities and programs. The planning estimate's total cost for project design, construction, furnishing, and equipping is $5,000,000.

The San Marcos Municipal Airport is in desperate need of an ARFF to enhance public safety and security. Both the City of San Marcos and the San Marcos Fire Department need a fire station to serve the expanding eastern section of the city. The Gary Job Corps Center needs a fire fighter and first responder training school. All these critical public policy needs can be most effectively and efficiently met with a multi-purpose fire station and fire fighter training facility located on the San Marcos Municipal Airport. This multi-purpose facility would maximize the use of

limited public safety tax dollars, and, consequently, makes sense from a public policy perspective.

We appreciate very much the Subcommittee's consideration of this request for $5,000,000 for the City of San Marcos for this important public safety and security project.

PREPARED STATEMENT OF THE COALITION OF NORTHEASTERN GOVERNORS

As the Subcommittee begins the fiscal year 2006 transportation appropriations process, the Coalition of Northeastern Governors (CONEG) is pleased to share with the Subcommittee testimony on the fiscal year 2006 Homeland Security Appropriations bill. The CONEG Governors commend the Subcommittee for its past support of funding for the Nation's critical transportation security needs, particularly rail security. Although we recognize the extensive demands being made upon Federal resources in the coming year, we urge the Subcommittee to continue the important Federal role in securing the Nation's transportation systems.

Efforts to strengthen the Nation's security, particularly its multi-modal transportation system, are of paramount importance to the CONEG Governors. We believe high priority must be given to the safety and security of the Nation's passenger rail systems, and therefore urge that the fiscal year 2006 Appropriations include the funding necessary to enable the Department of Homeland Security to help strengthen the security of the Nation's intercity, commuter rail, and rail transit systems. These extensive systems move millions of riders daily, and are critical components of the transportation network. Funding for rail security programs will allow the Department of Homeland Security to be an essential partner with States, local governments and public transportation authorities in ensuring that these vital rail systems remain accessible, reliable—and safe.

The CONEG Governors thank the entire Subcommittee for the opportunity to share these priorities and appreciate your consideration of these requests.

PREPARED STATEMENT OF THE GREATER ORLANDO AVIATION AUTHORITY

Chairman Gregg and distinguished members of the Senate Appropriations Subcommittee on Homeland Security: The Greater Orlando Aviation Authority ("the Authority") greatly appreciates the opportunity to submit written testimony in support of funding initiatives necessary to enhance the efficiency and execution of Department of Homeland Security requirements at Orlando International Airport. The Authority remains a steadfast partner in ensuring the highest standards of public safety and security of our homeland and deeply appreciates the leadership and efforts put forth by you and your Subcommittee to advance this mission.

The Authority respectfully requests your Subcommittee's consideration and support of the following Federal initiatives:

Integrated U.S. Customs and Border Protection (CBP)/USDA Animal and Plant Health Inspection Service (APHIS) Facility

Two years ago, our Nation took a bold advancement in border protection by unifying all Federal entities with border responsibilities under one frontline border agency—the U.S. Bureau of Customs and Border Protection (BCBP) within the Department of Homeland Security. Identified as "One Face at the Border", this historic initiative merged the personnel and functions of the former Customs Service, the Immigration and Naturalization Service, the Animal and Plant Health Inspection Service and the U.S. Border Patrol to enhance efficiencies and create greater accountability in one seamless border service. Today's CBP officers are cross-trained to perform all functions previously fulfilled by the individual legacy agencies.

On March 1, 2003, CBP designated a Port Director at each port of entry to implement a single, unified chain of command. At Orlando International Airport, an officially designated Port of Entry, over 230 employees of the legacy agencies were brought under the single command of our Area Port Director. Although functions have been merged to create a seamless border and inspection service, operational locations are still stretched across the airport's 13,247 acres at multiple locations.

The primary CBP facility, constructed almost a decade ago, is located on the west side of the airport in the Tradeport Drive area. As a result of the BCBP initiative, this facility is being utilized to its maximum capacity and does not have the flexibility to accommodate the realignment and future growth of staffing. INS functions are housed in an independent facility along the west side of the airport, as is the USDA Animal and Plant Inspection Service personnel.

The Greater Orlando Aviation Authority respectfully requests funding under the Department of Homeland Security to construct a 28,000 square foot companion facility adjacent to the existing CBP facility in order to promote a campus-style complex. This facility will accommodate capacity needed by CBP and bring existing APHIS staff and inspection facilities closer to CBP to increase interaction and accessibility. Such a facility will ensure improved communications and efficiencies needed to implement the Department's mission to protect the security of our borders and homeland.

The Authority respectfully requests the Committee to include the following line item in the fiscal year 2006 DHS budget:

"Design and Construction of an Integrated U.S. Customs and Border Protection/USDA APHIS Facility at Orlando International Airport—$9,000,000"

Additional U.S. Customs and Border Protection Staffing Positions

Orlando International Airport continues to steadily rebound from the events of September 11, 2001 and significantly outpace passenger growth estimates. During the past year, our airport has moved upward in performance rankings to now lead as the 12th busiest commercial passenger service airport in the Nation and the 20th busiest in the world. Orlando International Airport has also surpassed Miami International Airport as Florida's busiest commercial service airport.

As Orlando is a top destination choice of passengers, it is no surprise that Orlando International Airport also ranks as our Nation's 5th largest Origination and Destination (O&D) Airport. As O&D passengers are required to undergo more security screening requirements than connecting passengers because they enter the sterile security area for the first time, appropriate levels of staffing are needed to ensure the efficient and timely flow of passengers through the screening and inspection process.

CBP passenger wait times at Orlando International Airport routinely exceed the national average. Additional inspectors are needed to accommodate the airport's continuing growth. Annual CBP Inspector expenses are approximately $150,000 per inspector per year. Federal funding in the amount of $750,000 is needed to support the addition of five new CBP officers.

The Authority respectfully requests the Committee to include the following line item in the fiscal year 2006 DHS budget:

"Additional CBP staffing positions at Orlando International Airport—$750,000"

Installation of In-Line Checked Baggage Explosive Detection System (EDS)

Over 2 years ago, the Authority received concept approval from the Transportation Security Administration (TSA) for the installation of an In-Line Checked Baggage Explosive Detection System (EDS); however, the TSA has not issued a Letter-of-Intent to proceed with installation of this system due to lack of available Federal funding. Since the design has already been completed, the system could be installed and fully operational within two years if Federal funding is obtained.

Orlando International Airport (OIA) currently has 41 EDS machines located throughout the airport, with the majority in ticket lobbies and other passenger areas of the terminal. The physical size of each machine and the footprint support area consumes a significant portion (10 to 15 percent) of the terminal's capacity needed to process and move passengers efficiently. The airport has already implemented substantial renovations to the main terminal in partnership with the Federal Aviation Administration to maximize the flow and efficiency to the greatest extent possible. The existing placement of the EDS equipment negates the effectiveness of this substantial investment and may lead to the airport exceeding capacity levels earlier than projected.

Installation of an In-Line system would result in a significant reduction in the number of EDS machines needed and the number of personnel required to manual operate the integrated system. Of the 1,000 plus TSA personnel currently stationed at the airport, almost half (50 percent) are dedicated to the operation of the free standing EDS machines. Initial investments by TSA for in-line systems clearly result in immediate and long-term operational cost savings to the Administration.

OIA primarily serves origination and destination travelers, who undergo more screening requirements than connecting passengers. O&D passengers represent approximately 95 percent of all passengers at OIA. This high level of O&D activity is expected to continue. The Airport accommodates more leisure travelers, who typically travel with a greater number of bags and unusually-sized accompaniments such as golf clubs, water skis, surfboards, etc. Under the current system, passengers must wait in airline check-in lines to obtain a boarding pass; then carry their luggage to the nearest EDS machine. Overall, installation of an In-Line EDS at Orlando International Airport would result in significant operational cost savings for

TSA; recovered terminal capacity for the airport; and a return to customer-friendly expedited passenger processing. The total cost of the In-Line EDS Phase II System is estimated at $100 million.

The Authority respectfully requests the Committee to include additional funding for the installation of In-Line Checked Baggage Explosive Detection Systems to enable TSA to execute additional Letters of Intent to airports such as Orlando International Airport.

Justification and Closing

Orlando International Airport remains steadfast in its commitment to help our Nation in its mission to protect our borders and homeland while enabling safe, efficient and timely movement of passengers and commerce.

Orlando International Airport (OIA) is one of the Central Florida's primary assets and has been designated as an U.S. Security Category X airport. In 2004, OIA served approximately 31.1 million passengers, surpassing Miami International Airport as the busiest commercial passenger airport in Florida. Additionally, OIA is the 12th busiest commercial service airport in the Nation and the 20th busiest in the world. In terms of origin and destination (O&D) passenger traffic at domestic airports, OIA ranked 5th behind Los Angeles International and traditional airline hub airports such as Las Vegas' McCarran International, Atlanta's Hartsfield International and Chicago's O'Hare International. O&D passengers represent approximately 95 percent of all passengers at OIA. This high level of O&D activity is expected to continue.

OIA has scheduled service to 82 non-stop domestic destinations and 19 non-stop international destinations, promoting increased airline service and competitive fares. The largest rental car market in the world is located at OIA. The airport shares a unique relationship with the regional economy. A completed Economic Impact Study determined OIA generates a $20.7 billion annual economic impact on Central Florida and is responsible for 62,100 direct and indirect jobs.

The Authority expresses its gratitude for the opportunity to present this testimony to your Subcommittee. We look forward to working with you in advancing these safety and security initiatives that will benefit the National Aviation System.

PREPARED STATEMENT OF THE INTERNATIONAL ASSOCIATION OF EMERGENCY MANAGERS

Chairman Gregg, Ranking Member Byrd, and distinguished members of the Subcommittee, thank you for allowing me this opportunity to provide testimony on the President's fiscal year 2006 budget request for the Department of Homeland Security.

I am Dewayne West. As the Director of Emergency Services for Johnston County, North Carolina, I supervise the Emergency Management program, the Fire Marshal's Office and Emergency Medical Services. I currently serve as the President of the International Association of Emergency Managers (IAEM) and am providing this testimony on their behalf. I am also a Certified Emergency Manager (CEM), a member and past president of the North Carolina Emergency Management Association, and the Vice Chairman of the Emergency Management Accreditation Commission (EMAP). I was recently appointed by the Governor to serve on the N.C. State Emergency Response Commission (SERC).

The International Association of Emergency Managers has over 2,600 members including emergency management professionals at the State and local government levels, the military, private business and the nonprofit sector in the United States and in other countries. Most of our members are city and county emergency managers who perform the crucial function of coordinating and integrating the efforts at the local level to prepare for, mitigate the effects of, respond to, and recover from all types of disasters including terrorist attacks. Our members include emergency managers from large urban areas as well as rural counties.

We appreciate the support the Subcommittee has given to emergency management in the past 2 years and especially appreciate your support for the Emergency Management Performance Grants and your strong support for and the all hazards mission.

We respectfully request your assistance on two issues.

Emergency Management Performance Grants (EMPG)

—Request the $10,000,000 funding cut be rejected and the amount increased to $280 million to begin addressing the shortfall.

—Request that EMPG funding be maintained in a separate account as in the fiscal year 2005 Congressional action and not combined with other grant programs.

Hazard Mitigation Grant Program (HMGP)

—Request that the legislative language proposed in the budget to reduce the formula for States with enhanced plans from 20 percent to 12.5 percent be rejected.

—Request HMGP formula for States with basic mitigation plans be restored to 15 percent of FEMA eligible cost.

EMERGENCY MANAGEMENT PERFORMANCE GRANTS (EMPG)

Increase funding for EMPG.—Appropriations Committee report language referred to the program as "the backbone of the Nation's emergency management system." In order to maintain this system and build the capacity required to meet the greatly increasing demands, additional investment is needed.

However, the President's Budget request for fiscal year 2006 proposes to reduce the funding from the $180,000,000 appropriated in fiscal year 2005 to $170,000,000. According to a biennial study conducted by the National Emergency Management Association (NEMA) in 2004 there is a shortfall of $264 million. We respectfully request that EMPG be increased $100 million over the fiscal year 2005 level for a total of $280,000,000 to begin addressing this shortfall.

The Emergency Management Performance Grants (EMPG) constitute the only source of direct Federal funding for State and local governments to provide the foundation for basic emergency coordination and planning capabilities for all hazards, including those related to homeland security. The grants are pass through grants to State and local emergency management offices and are used predominately for personnel who plan, train, coordinate, and conduct exercises and other functions essential to effective preparedness, mitigation, response and recovery efforts.

EMPG grants require a 50 percent State or local match. Currently many local jurisdictions are receiving 20 percent or less. In addition many local jurisdictions receive no funding because of shortage of funds.

Natural disasters continue to remind us of the great need for preparedness and response coordination. In 2004 alone there were 68 federally declared disasters and 7 emergencies and local officials responded to many more disasters that were not federally declared. The size and scope of Hurricanes Charley, Frances, Jeanne and Ivan underscored the need for a strong national emergency system. Eight hundred personnel from thirty-eight States provided support to the affected States and communities through the Emergency Management Assistance Compact.

State and local emergency management programs are in desperate need of financial support if they are to continue to meet the requirements of all hazard planning and coordination as well as implement the President's homeland security strategy in States, counties, cities and neighborhoods across America. Emergency managers must meet the challenge of bringing the emergency response planning and organizations in their States and communities in line with new Federal requirements contained in the National Incident Management System (NIMS), the National Response Plan (NRP), and numerous new and pending national standards for preparedness and response.

The new security concerns arising from the current world situation make the coordination and unifying role served by emergency managers more important than ever. Given continued support and funding, emergency managers have the skills, the expertise, and the willingness to rise to the planning and coordinating challenges presented by the full range of hazards affecting their communities.

Maintain EMPG as a separate account.—We also urge you to continue to maintain EMPG as a separate account. The President's budget includes this program in the "State and Local" account with a number of other grant programs. EMPG is different from the other programs in this account. EMPG has existed for over 50 years and supports all hazards emergency management, including terrorism. In addition, it is a performance based continuing program with deliverables and requirements which must be met in order to receive funding the next year.

HAZARD MITIGATION GRANT PROGRAM (HMGP)

The Hazard Mitigation Grant Program which is authorized by Section 404 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act provides funding to States following a Presidentially declared disaster in an amount equivalent to a percentage of eligible FEMA funds. The monies are provided by the President's Disaster Relief Fund and the costs are shared 75 percent Federal and 25 percent State

or local. These funds are critical to reducing the costs and impacts of future disasters by breaking the cycle of damage and repair and damage again.

Reject funding cut for States with enhanced plans.—The fiscal year 2006 budget request in the Disaster Relief account in the Emergency Preparedness and Response Directorate proposes the following legislative language which would amend the Stafford Act: Provided, that the post-disaster hazard mitigation set aside for States is 7.5 percent of eligible disaster costs: Provided further, That States with an Enhanced Mitigation Plan may receive up to 12.5 percent of eligible disaster costs.

This language would reduce funding available for post disaster mitigation to States with approved enhanced mitigation plans from an amount equivalent to 20 percent of eligible FEMA disaster costs to only 12.5 percent. Since the passage of the Disaster Mitigation Act of 2000 which added the 20 percent incentive, FEMA has strongly encouraged States to work toward these enhanced plans. The FEMA regulations stated "A State with a FEMA approved Enhanced State Mitigation Plan at the time of a disaster declaration is eligible to receive increased funds under the HMGP, based on 20 percent of the total estimated eligible Stafford Act disaster assistance." The States of Missouri, Oklahoma, and Washington have achieved this goal and others have been diligently working toward it. This effort required a very significant commitment of resources from already overburdened State and community officials to develop a comprehensive mitigation program and requires States to take on significant additional responsibility. However, many States have committed to the additional effort because of the 20 percent incentive provided by Congress. The "carrot" of increased funding has been in the law over 4 years. Now that States have made the effort to achieve the goal, the Federal commitment should be kept. We urge you to reject the language lowering the percentage for States with Enhanced Mitigation Plans.

Restore Hazard Mitigation Grant Program (HMGP) to 15 percent.—The President's budget language continues the HMGP program at 7.5 percent. The fiscal year 2003 Omnibus Appropriations bill changed the formula used to determine hazard mitigation funding from 15 percent to 7.5 percent of eligible disaster costs and provided funds for a new nationally competitive predisaster mitigation grant program. Citizens and elected officials are most receptive to undertaking projects and initiatives that prevent the loss of life and reduce destruction of property immediately after a disaster has occurred. States and communities regularly report that the demand for post-disaster grants exceeds the available funding. Now, with the HMGP funding reduced by half, many more of these post disaster opportunities are being missed. We urge you to restore HMGP to 15 percent.

Thank you for giving us the opportunity to provide this testimony. We would welcome the opportunity to provide additional information to the Subcommittee.

PREPARED STATEMENT OF THE NATIONAL EMERGENCY MANAGEMENT ASSOCIATION

INTRODUCTION

Thank you Chairman Gregg, Ranking Member Byrd, and distinguished members of the Committee for allowing me the opportunity to provide you with a statement for the record on the Department of Homeland Security (DHS) fiscal year 2006 budget. I am David Liebersbach, the President of the National Emergency Management Association and Director of the Alaska Division of Homeland Security and Emergency Management. In my statement, I am representing the National Emergency Management Association (NEMA), whose members are the State emergency management directors in the 50 States, the U.S. territories, and the District of Columbia. NEMA's members are responsible to their governors for emergency preparedness, homeland security, mitigation, response, and recovery activities for natural, man-made, and terrorist caused disasters.

Over the past year, our Nation's emergency management system has been tested by the extensive natural disasters that we have faced. In all, there were 68 major disaster declarations, seven emergency declarations, and 43 fire management assistance declarations. Our Nation bravely faced and responded to one of the most active hurricane seasons with impacts by tropical Storm Bonnie, Hurricanes Charley, Frances, Gaston, Ivan and Jeanne, while also dealing with other disasters like flooding, tornadoes, and earthquakes. We also watched the aftermath of the tsunami in the Indian Ocean and saw graphically illustrated the importance of catastrophic disaster planning and maintaining our own emergency preparedness and response system. In Alaska, we experienced the largest fire season ever, with fires impacting over 6.5 million acres and 10,000 square miles. At the same time, emergency management continues to prepare for the threat of terrorism with new requirements

coming from the Federal government such as updating State plans to reflect the National Response Plan (NRP), training emergency responders on the new National Incident Management System (NIMS), and implementing the National Preparedness Goal mandated by Homeland Security Presidential Directive 8 (HSPD 8) on National Preparedness with no additional Federal financial assistance to meet Federal mandates. The multi-hazards emergency management system continues to be the means to practice and exercise for devastating acts of terrorism, while at the same time preparing the Nation for hurricanes, tornadoes, hazardous materials spills, and floods. We respectfully ask for your Committee to consider the role of emergency management as you address the fiscal year 2006 appropriations.

All-hazards preparedness is in danger of being regarded as a thing of the past as more focus is being placed on terrorism. We must ensure that our capability to deal with many hazards, including terrorism remains intact and that we do not shift our focus to preparedness for a single peril. The capability to coordinate an effective response to an event does not change by the type of disaster. The HSPD 8 process shows the increased focus on terrorism with only 2 of the 15 disaster scenarios representing traditional natural disasters. The all-hazards approach relies upon the maintenance of plans, trained personnel to carry them out, and supporting infrastructure in the form of emergency operations facilities with inter-operable communications. We must continue this approach in practicing and exercising for all emergencies, to include devastating acts of terrorism, as well as day-to-day emergencies. We cannot afford to lose the system we have in place to deal with all disasters in order to build new infrastructure for homeland security's sake.

The Department of Homeland Security budget provides critical support to State and local emergency management programs through actual dollars, grants, and program support. This year, NEMA would like to address three main issues with the proposed Federal budget for Department of Homeland Security.

—Extreme concern for proposed cuts to the Emergency Management Performance Grant (EMPG) program while requirements increase for State and local governments;
—The need to address massive shortfalls in updating Emergency Operations Centers (EOCs); and
—Concern about the reduced formula for the post-disaster Hazard Mitigation Grant Program (HMGP).

EMERGENCY MANAGEMENT INFRASTRUCTURE FUNDING

The Emergency Management Performance Grant (EMPG) is the only all-hazards emergency preparedness grant program in support of capacity building at the State and local level. At a time when we are aiming to build the system, additional resources and funding is needed to sustain State and local emergency management. The State and local government partnership with the Federal Government to ensure preparedness dates back to the civil defense era, yet increased responsibilities over the last decade have fallen on State and local governments. With the recent expanded focus on terrorism and the increased demands of the Federal Government to assist in implementation of Federal initiatives like the NRP, the NIMS, and HSPD 8, EMPG becomes more important as a means to ensure State and local involvement and compliance with new systems.

The President's budget proposal will have a devastating impact on the Nation's emergency management system at the same time that responsibilities are increasing for new and emerging hazards. The proposal decreases funding for the EMPG program by $10 million. These cuts mean that emergency management would be saddled with increased mandates, while coping with decreases to an already modest budget. In budget consideration for fiscal year 2003 and 2004, Congress has affirmed the importance of EMPG in appropriations bills in language addressing the significance of the program and increased the levels of funding for the program twice. Prior to these increases in fiscal year 2003 and 2004, the program had been straight lined for over a decade. Additionally, Congress affirmed the intent of the program as all-hazards and dedicated to supporting personnel during consideration of the fiscal year 2005 budget. NEMA is appreciative of Congress' recognition of the EMPG program, but this year we respectfully ask that Congress aggressively address the programs shortfalls with an additional $100 million in funding for EMPG for fiscal year 2006.

EMPG is the only all-hazards program that State and local governments can use to build their emergency management capacity. The grants can be used for personnel, planning, training, exercises, warning systems, emergency operations centers, public outreach, and interagency coordination. EMPG is a flexible program that allows State and local governments to tailor funds to address the specific risks

and needs of their jurisdiction. While it is called a grant, EMPG is really a 50/50 cost-share system which ties together the emergency management system of local, State, and Federal Governments. Every dollar contributed by the Federal Government is doubled with State and local contributions. EMPG's modest Federal increases in 2003 and 2004 helped the program grow, but shortfalls continue to force an unequal burden on state and local governments. States are continuing to increase their out of pocket costs in order to ensure there is adequate funding for local programs. In fact, a 2004 NEMA study found that there is approximately a $264 million shortfall in EMPG for all 50 States. This means that many communities that would like to implement a full-time, professional emergency management capability cannot do so because of shortfalls in Federal funding. Further, EMPG is primarily used as a pass-through program for local governments, so the shortfall affects our smallest localities that are often those most in need of emergency preparedness planning. Currently, States and local governments are over matching the Federal Government's commitment to national security protection through EMPG by $96 million according to the same 2004 NEMA study.

During last year's hurricane season, the interdependencies of the Nation's emergency management system were tested through the Emergency Management Assistance Compact (EMAC). The state-to-state mutual aid compact enabled 38 States to provide assistance in the form of more than $15 million in human, military, and equipment assets and over 800 personnel to support the impacted States for over 85 days of continuous response operations. The nature of the Nation's mutual aid system vividly shows the need for all States to have appropriate capabilities for all disasters. Additionally resources are needed to build emergency response capabilities on a national basis and to ensure the system can handle the demand of natural disasters and other emergencies no matter where they occur. EMPG is the only means to support this assistance that can be offered by other States in the face of disaster through adequate preparedness. EMPG ensures all States have funding to develop and maintain a base level capacity that can be utilized by other States for mutual aid.

While terrorism continues as a major focus at this time, we must balance preparedness efforts by integrating terrorism as one of the many threats facing our Nation, rather than the current approach of making all other preparedness efforts a subset of terrorism. Further, Homeland Security Presidential Directive 8 States that, "to the extent permitted by law, Federal preparedness assistance will be predicated on the adoption of statewide comprehensive all-hazards preparedness strategies." The all-hazards approach cannot be dismissed based upon the assumption that one threat is greater and more significant than the other. After all, no one really has a crystal ball to predict what the next disaster or emergency may be. Yet, the Federal requirements tied to homeland security are not funded. Focus and resources will have to be taken away from other preparedness initiatives in order to address these new demands. Our system for day-to-day public safety and homeland security must be mutually supportive and nimble enough to address any hazard.

Last year, Congress affirmed the Department of Homeland Security's (DHS) intent to create a "one stop shop" for homeland security funding. As the fiscal year 2005 funding has been processed, NEMA has been working alongside the Office of State and Local Coordination and Preparedness (OSLCP) to ensure that the all-hazards intent of the program is not changed. Additionally, OSLCP is looking at ways to improve the program also in coordination with NEMA. However, because DHS is a new Department with a new and developing financial management system the changeover has not been without significant delays in the amount of time that it takes for States to get their funding. In fact, homeland security funding including EMPG is processed through the legacy Department of Justice system that was used before the Office for Domestic Preparedness was transferred into DHS. Additionally, integrating EMPG funding into the homeland security grant program means that in more than half of the States, another layer of bureaucracy is added because only half of the Nation's emergency managers serve as the State administering agency (SAA). In these cases, it takes even longer for emergency management agencies to access the EMPG funding once it is awarded. This has a domino effect as delays are then experienced by local governments that receive EMPG monies. NEMA has received reports of situations in which county emergency management programs were on the verge of shutting their doors because they had expended their match funds while Federal funding continued to lag. In most States, EMPG funds were not received until 6 months into the Federal fiscal year. NEMA hopes to work collaborately with Congress and OSLCP to resolve these issues in the coming year to ensure swifter grant awards in fiscal year 2006. Specifically, we ask that Congress de-couple the Emergency Management Performance Grant which is an all-haz-

ards, 50/50 match program from the homeland security grant program which is terrorism focused with different and longer-term requirements.

The Federal Government must continue the commitment to ensuring national security though all-hazard preparedness. Without adequate numbers of State and local personnel to operate the all-hazards emergency management system, the infrastructure used to prevent, prepare for, respond to, and recover from all disasters will collapse. Congress must ensure predictable and adequate funding levels for the program.

EMERGENCY OPERATIONS CENTERS

Emergency Operations Centers (EOCs) serve as the nerve center as well as the State and local government coordination point during disasters and emergencies. In fiscal year 2002 and 2003, a total of $81 million was appropriated to the Federal Emergency Management Agency to address Emergency Operations Centers (EOCs) improvements. The $81 million was allocated to States to begin the planning process to assess the necessary infrastructure and security improvements and security measures to be taken. Since then, no dedicated Federal funding has been provided for the implementation of these plans. Many State and local facilities are out of date; do not have the interoperable technology to coordinate with the Federal Government or among State and local levels; and lack adequate security features. Federal assistance is necessary to match State and local commitments to upgrade their EOCs as an integral part of the Nation's emergency response system. According to a 2004 NEMA survey, it is projected that more than $1.6 billion will be needed to construct and maintain State and local primary and alternate EOCs over the next 2 to 5 years. This includes the costs to consistently upgrade equipment, buildings, and software, train personnel, and conduct operations during emergency and non-emergency situations. NEMA calls on Congress to assist in addressing this shortfall and immediate need. When Congress did begin to address this shortfall, the match requirement was lowered to 25 percent for State and local governments. Congress should make a $160 million commitment this year as a down payment to addressing the shortfall, or EOCs will fall further behind.

HAZARD MITIGATION GRANT PROGRAM & PREDISASTER MITIGATION

NEMA supports efforts by the Congress and the Administration to continue both pre- and post-disaster mitigation activities. NEMA calls on Congress to restore the post-disaster Hazard Mitigation Grant Program (HMGP) formula to 15 percent and maintain the formula at 20 percent for "enhanced plan" States. Disasters present the opportunity to learn from past mistakes and to also take advantage of the lessons learned during the disaster. This means funding for utilizing elevations and buy-outs as tools and building warning systems and shelters.

Effective February 20, 2003, Congress changed the formula for post-disaster mitigation grants from 15 percent to 7.5 percent. This change limits the availability of funds for post-disaster mitigation and prevents the lessons learned from disasters from being immediately incorporated into mitigation projects to prevent loss of life and destruction of property. The months immediately following disasters provide unique opportunities to efficiently incorporate risk reduction measures in a very cost-effective manner, in many cases lowering the overall cost of the project by leveraging other funding sources including insurance settlements. We ask that you restore the formula to 15 percent this year in order to address mitigation needs.

This year, the Administration is proposing to decrease the post-disaster formula for "enhanced plan" States as well. Last year, all States were required to complete hazard mitigation plans and to have them approved by the Federal Emergency Management Agency (FEMA). As a result of changes made to the Stafford Act in the Disaster Mitigation Act of 2000, States could opt to do more work and planning in order to qualify for enhanced plans. Thus far, three States (Missouri, Washington, and Oklahoma) have qualified to receive the 20 percent formula as enhanced plan states, and many more States are pursuing enhanced plans for approval. But, the Administration is proposing to lower the enhanced plan formula to 12.5 percent of disaster costs, reducing the incentives for States to make the investment to seek enhanced plans. Further, this will limit even more the mitigation opportunities that are addressed in disaster-prone States.

The HMGP has proven to be a highly effective tool in steering communities toward risk reduction measures, in many cases breaking repetitive loss cycles that have cost other Federal disaster relief programs multiple times. Cost-benefit analysis is currently a requirement for predisaster mitigation programs. We must not lose these opportunities to initiate projects to enhance our communities and reduce

future disaster costs. HMGP must be restored and the enhanced plan formula must be maintained.

HOMELAND SECURITY GRANT PROGRAM

Congress has made significant attempts to ensure that the Homeland Security Grant Program is streamlined and provides greater flexibility. We appreciate the attention and funding that the Congress has given to ensuring emergency responders are adequately prepared for domestic terrorism threats. Emergency responders are better prepared today to face the various threats associated with terrorism because of the Federal commitment to address the war on terrorism that is being played out in our States, cities, and towns. States continue to take an all-hazards approach to disaster preparedness as we have integrated our domestic preparedness efforts into the proven systems we already use for dealing with both man-made and natural disasters.

Funding Levels

We continue to be concerned about cuts in the President's budget proposal for homeland security that has been dedicated to improving emergency responder preparedness for homeland security. The Federal Government must maintain its commitment to ensure that homeland security preparedness continues and the Constitutional responsibility to maintain a national defense is not compromised. Continuity of effort can only be maintained by State and local governments with adequate Federal support, especially when it deals with the front line emergency responders. Reductions in funding will immediately be translated into reductions in prevention, protection, and preparedness activities. Regional collaboration and mutual aid are critical components of the National Preparedness Goal. If the Federal Government provides adequate funding to the States for the necessary resources to be put in place to respond to any event, then the Federal Government is supporting one of the key overarching goals of the National Preparedness Goal. Further, continued or increased funding should not take away from traditional all-hazards capacity building programs for public safety, public health, and emergency management.

Congressional Legislation to Simplify the Grants Process

As Congress considers legislation to address and reform the Homeland Security Grants, we ask that you take NEMA's suggestions into consideration. The suggestions include the following:

—Each State must have a base minimum level of funding to ensure the capacity to respond to any event. Such capacity is necessary for homeland security because of the changing nature of the threat and also because of the importance our emergency system places on mutual aid to respond to events;

—All efforts to increase emergency management capacity must be coordinated through the States to ensure harmonization with the State emergency operations plan, ensure equitable distribution of resources, and to synthesize resources for intra-state and inter-state mutual aid. Also, the Stafford Act, which governs the way disaster assistance is allocated, successfully uses States and Governors as the managers of Federal disaster relief funds for local governments, which can become overwhelmed and in need of assistance when disasters occur.

—States understand the need to get funding quickly to the first responders and have long coordinated statewide and regionally to ensure adequate State assistance to local governments for emergency preparedness and response; and

—Traditional emergency management capacity building programs like EMPG must be continued as separate and distinct from the homeland security grants programs.

Fiscal Conditions and Match Requirements

Further, because the war on terrorism is a national emergency and States and local governments continue to be in the toughest fiscal situations since the deep recession in the early 1980s, we must be wary of programs that would require significant matches. In fact, for local governments to meet the match would be even more difficult given their fiscal constraints. If a significant match is required, the application of this initiative will only go to those agencies and governments that can fiscally afford the match and not necessarily where the need is greatest. If a match is necessary, we would suggest that the match be non-fiscal or in the form of a deliverable as opposed to soft or hard dollars. Waivers may be a way for the Federal Government to also address the lack of capital for a match when State and local governments are experiencing fiscal distress.

Flexibility for Personnel to Manage the Program

Greater flexibility to use some of the first responder grants for personnel both at the State and local level to manage the programs is critical to completing the preparedness mission. As an existing funding stream, EMPG is used in part to fund State and local staff to manage critical programs including the homeland security grants. The First Responder Grants should recognize that personnel are necessary to manage these programs, particularly when rigid deadlines are set for obligating millions of dollars and accountability is paramount. Additionally, new needs such as intelligence fusion personnel must be recognized. As HSPD 8 deadlines loom, States will be faced with a new set of requirements that could be tied to funding. Simply hiring contractors to do the work is not a long-term solution for building and maintaining national preparedness capabilities. State and local government, emergency management, and responder organizations are already working at a maximum capacity within existing resources and need Federal support for more than the purchase of equipment and exercises. Flexibility based on strategic approaches should be the norm, not single-issue, narrowly focused grants.

NATIONAL HOMELAND SECURITY CONSORTIUM

The National Homeland Security Consortium is a voluntary, education and outreach group representing State homeland security advisors, State and local law enforcement, emergency management, fire, public health, EMS, National Guard, public works, emergency communications, State and local elected officials and private sector partners. The Consortium was established in 2003 by the National Emergency Management Association and was endorsed by former DHS Secretary Tom Ridge in September 2004. This comprehensive group of subject matter experts offers itself as a technical resource and sounding board for the Department of Homeland Security as they develop and implement new policies and programs. The Consortium represents State and local officials on the ground, in city hall and in the statehouses charged with the responsibility of homeland security and overall public safety. The group is meeting again in May to provide another opportunity for all disciplines and levels of government involved in emergency prevention, preparedness, response and recovery to come together to continue to share information, develop solutions to common challenges and build relationships that will enhance State and local homeland security capabilities. The Consortium serves as a model for intergovernmental coordination and demonstrates the commitment of State and local governments to collaboratively address the complex challenges of homeland security.

CONCLUSION

While we as a Nation are fortunate that another year has passed without a terrorist incident on our Nation's soil, we must continue to build national preparedness efforts with a multi-hazard approach. We must be prudent and thoughtful in addressing homeland security enhancements to our existing emergency preparedness and response system. In this year's appropriations process Congress will make critical decisions that shape the future of emergency management in this country. As you begin your consideration, we ask you to recognize the importance of adequately funding the EMPG program in building capacity through people at the State and local level for all disasters. I thank you for the opportunity to testify on behalf of NEMA and appreciate your partnership.

PREPARED STATEMENT OF THE NATIONAL FLOOD DETERMINATION ASSOCIATION

Mr. Chairman and members of the Subcommittee, the National Flood Determination Association (NFDA) strongly supports the Budget Request for the Flood Map Modernization Presidential Initiative. This major project to update and modernize the Nation's flood risk maps is critical to the functioning of the National Flood Insurance Program (NFIP) and to protection of property through effective floodplain management.

The NFDA is a professional association of companies which provide flood zone determinations to lenders for compliance with the mandatory purchase requirements of the NFIP. The association represents some two thirds of the industry and has implemented a certification program containing standards for flood zone determination companies. Because the FEMA flood maps are the official documents for compliance with the NFIP, flood determination companies are probably the most frequent users of the maps. A survey of the NFDA membership reveals that it has completed approximately 33,000,000 determinations in the year 2003.

Flood maps are used both to determine which properties are in or out of a Standard Flood Hazard Area (SFHA) and also are used by county and community officials to plan development and to reduce future risk.

Approximately 70 percent of the maps are 5 years and older, 45 percent at least 10 years old, and more that 2,200 flood prone communities remain without flood hazard maps. The current process utilized by FEMA to produce an updated map is 58 months. More than 20,000 map panels identified as requiring updates, meaning they have outdated or inadequate flood hazard data requiring updates through field reconnaissance, engineering analysis and floodplain mapping utilizing improved analysis methodologies. The detailed flood studies will include "approximately studied" and "unstudied" flood-prone communities. There are more than 40,000 maps with adequate flood hazard data but inadequate non-engineering data and reference features such as roads. New elevation reference marks will be developed and implemented emphasizing the use of GPS surveying technology and a network of approximately 580,000 benchmarks.

Complaints to lenders, flood determination companies, and realtors dramatized the problems caused for real estate transactions when maps do not reflect true risk. Over a 10 or 20 year period, development, road building and re-grading of land significantly alter flood risk.

The NFDA has been extremely gratified that the Administration has recognized the real need to update and modernize the flood maps. As the Map Modernization project develops, however, we have some concerns about the update component. Updating the maps, particularly in high growth areas, requires a full restudy which includes engineering, surveying, hydrology and hydraulics. It should be noted that such extensive restudy is not needed everywhere as the water flow and retention properties may not have changed much over the years. Because the updates require more time and investment, we are worried that insufficient analysis is being undertaken in order to complete action on maps more quickly. The quantitative requirements by which the map modernization is judged may be moving away from the restudies and toward limited revisions and digitization. Such a newly issued map, with a new date, can be very misleading. Flood determinations done using these "new" maps will continue to generate complaints.

To do justice to the national investment in good flood risk maps, there may need to be some adjustment to the quantitative standards by which the program is evaluated. It may not be possible to complete the job in the originally projected 5 years.

Some technical coordination issues have also become apparent. It is key that the map modernization process and product reflect the needs and requirements of map users. For this reason, we strongly urge the establishment of a stakeholder advisory group. This could be modeled on the successful Technical Mapping Advisory Board established for 5 years by the Flood Insurance Reform Act of 1994. It is our understanding that FEMA has been looking into creating this kind of advisory board. We urge the Committee to support this effort.

We were aware of a possibility last year that certain (at the time) funds not obligated to map modernization could be redirected to other needs of the Department of Homeland Security. Because it is becoming very clear that the Nations' flood map modernization needs are extensive, we are concerned about any redirection of funds appropriated for the Flood Map Modernization Initiative.

The National Flood Determination Association remains committed to working with FEMA to achieve the updated, modernized national flood risk maps we all need. We urge the Committee to approve the full budget request of $200 million.

PREPARED STATEMENT OF THE OHIO DEPARTMENT OF CHIEFS OF POLICE, INC.

Chairman Gregg, Ranking Member Byrd and Distinguished Members of the Subcommittee, thank you for the opportunity to provide a statement for the record regarding the fiscal year 2006 budget proposal for the Department of Homeland Security.

Our names are Director Kenneth L. Morckel, Ohio Department of Public Safety and Director Todd N. Wurschmidt, Ph.D., Ohio Association of Chiefs of Police (OACP). Director Morckel is the designated head of Homeland Security efforts in Ohio as appointed by Governor Bob Taft. Dr. Wurschmidt oversees staff operations for the OACP and is involved in managing the statewide effort and information sharing between Ohio law enforcement agencies.

We respectfully request consideration on restoring a separate line item in Homeland Security funding for the category, "LETPP—Law Enforcement Terrorism Prevention Program." Highlights of our statement include:

—Prevention, Such As Information Sharing, Involves 100 percent of America's Law Enforcement Agencies
—Terrorists Can Plan Anywhere, Thus Involving 100 percent of America's Geography
—Preventing Terrorism Is Not UASI[1] Urbans Versus SARASI[2] Suburban and Rurals
—Law Enforcement's Prevention Role Should Not Be Formula Funded At the Expense of Law Enforcement's First Responder Role
—Proposed fiscal year 2006 Budget Cuts For Suburban and Rural Prevention and Responder Efforts Total 32 percent

Have you heard of Iyman Faris? Probably not. In 2003, Mr. Faris was making plans to blow up the Brooklyn Bridge. He was NOT living in Manhattan. Mr. Faris was apprehended outside of Columbus, Ohio. Had the Brooklyn Bridge gone down, we probably would have all known Mr. Faris's name well.

Heard of Azmi Al-Jayyusi? Probably not. In 2004, Mr. Al-Jayyusi headed up a sophisticated plot, designed in the small villages in Jordan, in which trucks, chemicals and explosives were surreptitiously purchased for purposes of blowing up select strategic targets (including the American Embassy) in the capital of Jordan, Amman. It was estimated the chemical explosives would have caused the deaths and injuries of 250,000 civilians. Once again, the urban city was not Mr. Al-Jayyusi's site for plotting and preparing; it was the rural countryside. Had Mr. Al-Jayyusi's terrorist plot been successful, we could probably recite his name easily as well.

Heard of Ted Kazenski, the Unabomber? Yes, of course. Why? Because this domestic terrorist was successful in reeking widespread fear, his deeds carried out from the isolated forests of rural Montana. How about Eric Rudolph, the Abortion Clinic Bomber? Yes? Mr. Rudolph's eventual capture occurred during late night, at the site of a trash bin, behind a business in the small North Carolinian town of Murphy; a rural apprehension.

"All across our Country we'll be able to tie our terrorist's information to local information banks so that the front line of defeating terror becomes activated and real, and those are the local law enforcement officials. We expect them to be part of our effort; we must give them the tools necessary so they can do their job." President George W. Bush, February 2003

As President Bush so accurately notes, preventing domestic and international terrorism requires enlisting the commitment and involvement of 100 percent of America's geography and 100 percent of America's law enforcement agencies.

Geography.—In the United States, there are 3,042 counties. There are only 60 to 65 counties within the UASI (Urban Area Security Initiatives) areas as designated by the U.S. Department of Homeland Security (Map 1). That leaves some 2,980 counties within the non-UASI, non-urban areas involved in preventing, detecting, deterring and disrupting terrorism (Map 2).

Successful terrorism prevention requires that these 2,980 SARASI counties (Suburban and Rural Area Security Initiatives) continue to receive LETPP[3] funds commensurate with their percentage geography, and commensurate with the need to prepare, equip and train all local law enforcement, urban, suburban and rural.

L/E Agencies.—This Nation's terrorism fight requires our enlisting the aid and commitment of all of America's 19,000 law enforcement agencies. Over 80 percent of U.S. law enforcement agencies are located outside the UASI cities, and within the SARASI counties, towns and villages. Less than 20 percent of America's law enforcement agencies are in UASIs. Yet, proposed fiscal year 2006 prevention funding is weighted toward 50 large cities and decreases funding allocations available to the over 80 percent of America's suburban and rural law enforcement agencies (Table 1).

TABLE 1.—UASIS[4] VERSUS SARASIS[5] IN PREVENTING, DETECTING, DETERRING AND DISRUPTING DOMESTIC AND INTERNATIONAL TERRORISM

[Prevention (E.G. Information Sharing) Involves 100 Percent of U.S. Law Enforcement Agencies]

	Total U.S.	UASIs	SARASIs
Counties:			
Number	3,042	60–65	2,980

[1] USAI=Urban Area Security Initiative.
[2] SARASI=Suburban and Rural Area Security Initiative.
[3] LETPP=Law Enforcement Terrorism Prevention Program.

TABLE 1.—UASIS[4] VERSUS SARASIS[5] IN PREVENTING, DETECTING, DETERRING AND DISRUPTING DOMESTIC AND INTERNATIONAL TERRORISM—Continued

[Prevention (E.G. Information Sharing) Involves 100 Percent of U.S. Law Enforcement Agencies]

	Total U.S.	UASIs	SARASIs
Percent	100	2	98
Law Enforcement Agencies:			
Number	About 19,000	About 3,500	15,500
Percent	100	18	82

[4] UASI=Urban Area Security Initiative.
[5] SARASI=Suburban and Rural Area Security Initiative.

"Preventing terrorism equates to intelligence" (eg. information sharing). Congressman Christopher Cox (R-CA), Chair, Homeland Security Committee, U.S. House of Representatives, February 2005.

In fiscal year 2004, the President and Congress identified the unique role of law enforcement in the Nation's fight against terrorism. That unique role of law enforcement is prevention. Thus, within the U.S. Department of Homeland Security's grant programs, the "Law Enforcement Terrorism Prevention Program" (LETPP) was created. In the above television interview, Chairman Cox emphasized the need for prevention, intelligence and information sharing. Prevention, intelligence and information sharing can only be achieved with 100 percent involvement of America's law enforcement agencies.

Although the proposed fiscal year 2006 President's budget collapses grant fund categories and incorporates LETPP funding into UASI and SHSGP[6] categories, the loss of the separate LETPP funding category will:

—Greatly restrict suburban and rural law enforcement from moving forward on prevention efforts such as information sharing;
—Increase the likelihood that local law enforcement will not be fully funded on prevention plus their responder roles because of the funding needs by all other public safety first responder and health agency groups; and
—Greatly restrict funding for law enforcement's responder roles because of formula funding that could be interpreted as having funded law enforcement because of the 20 percent prevention mandate.

Below we offer explanations for these potential complications.

"Smaller States would see an 80 percent cut according to the proposed fiscal 2006 budget. That's not just a small drop. That's a leap off the cliff." Senator Susan Collins (R-Maine), Chair, Senate Homeland Security and Governmental Affairs Committee.

The four-fold purposes of this document are to respectfully request the U.S. Congress:

—Reinstate the Homeland Security funding category of "LETPP—Law Enforcement Terrorism Prevention Program" as a separate line item funding category;
—Restrict the use of formula funding to require a threshold percentage of funding be directed toward prevention versus response efforts;
—Avoid funding allocations that will have UASI urban cities funded to the detriment of all other counties, towns and villages involved in the prevention of terrorism; and
—Avoid melding the prevention plus responder roles of law enforcement into one funding category used to fund responder functions for all other first responder public safety and health agency forces.

The original purpose of the fiscal year 2004 LETPP was to "seek to provide law enforcement communities with enhanced capabilities for detecting, deterring, disrupting, and preventing acts of terrorism."[7] It should be noted that the mission statement identified "law enforcement communities," not just urban area law enforcement communities.

The LETPP program funding category provided law enforcement communities with monies to pursue five program areas: (1) information sharing; (2) target hardening; (3) threat recognition; (4) intervention activities; and (5) interoperable communications.

The President's 2006 Proposed Budget from the U.S. Department of Homeland Security will inhibit efforts to build forward on terrorism prevention and first responder work of local law enforcement officials. The program budget review docu-

[6] SHSGP=State Homeland Security Grant Program.
[7] Fiscal year 2004 Homeland Security Grant Program: Program guidelines and application kit, U.S. Department of Homeland Security, page 38.

ment for fiscal year 2006 "State Homeland Security Grants Program" (as prepared by the Office of State and Local Government Coordination and Preparedness, U.S. Department of Homeland Security) shows a total appropriation budget request of $1.242 billion or, a $482 million reduction from the $1.725 billion homeland security funds approved for fiscal year 2005.8 This loss of half a billion dollars from thousands of public safety agencies' budgets will greatly reduce suburban and rural terrorism prevention and first responder efforts (Table 2 and Table 3).

The philosophical and strategic argument for increasing funds for the Nation's UASIs (Urban Area Security Initiatives) appears to involve the adoption of "risk assessment" as opposed to population formula for allocation of Homeland Security funds. The argument being put forward is that the major cities will, in greater probability, be the location of future terrorist attacks. Then, the argument of logic is furthered that these major urban centers need more monies to adequately prepare to prevent and respond. This argument should also recognize the significant role that all of this Nation's law enforcement agencies play in prevention efforts—to "detect, deter, disrupt and prevent acts of terrorism."

TABLE 2.—PROPOSED $480 MILLION (32 PERCENT) LOSS IN PREVENTION AND RESPONDER FUNDING FOR THE 2,980 SARASI [9] COUNTIES

[All suburban and rural prevention and responder efforts by fire, EMS, EMA, health and police will experience a 32 percent total cut in fiscal year 2006]

[In millions of dollars]

	Fiscal year 2005 enacted	Fiscal year 2006 request	Change
SHSGP [10]	1,100	1,020	(80)
LETPP [11]	400		(400)
Total Funding to Suburban & Rural SARASIs	1,500	1,020	(480) (32 percent cut)

[9] SARASI=Suburban and Rural Area Security Initiative.
[10] SHSGP=State Homeland Security Grant Program.
[11] LETPP=Law Enforcement Terrorism Prevention Program.

TABLE 3.—WITH THE PROPOSED FISCAL YEAR 2006 20 PERCENT FORMULA FUNDING FOR LETPP [12], FUNDING FOR JUST RESPONSE EFFORTS BY SUBURBAN AND RURAL PUBLIC SAFETY FORCES WILL BE CUT BY ($284 MILLION) (26 PERCENT CUT) FROM FISCAL YEAR 2005

[Proposed fiscal year 2006 First Responder cuts to SARASIs amount to a 26 percent cut from fiscal year 2005 funding levels]

[In millions of dollars]

	Amount		Amiount
Fiscal year 2006 Request SHSGP [13]	$1,020	SARASI First Responder fiscal year 2005	$1,100
Formula Funding percent to LETPP	204	SARASI First Responder fiscal year 2006	816
Balance to First Responder SARASIs [14]	816	Loss to SARASI First Responders	(284)

[12] LETPP=Law Enforcement Terrorism Prevention Program.
[13] SHSGP=State Homeland Security Grant Program.
[14] SARASI=Suburban and Rural Area Security Initiative.

Prevention of terrorism needs the involvement of 100 percent of the law enforcement community throughout the Nation. Although the probability of a future terrorist attack may involve major urban areas, the prevention of future terrorist attacks must involve all 19,000 law enforcement agencies throughout the 3,042 counties in the United States.

Information Sharing as Prime Example: Information sharing amongst law enforcement agencies is as critical as President Bush noted in his February 2003 comments noted earlier, and as reinforced by U.S. House Homeland Security Chair Congressman Cox's February 2005 comments noted previously. Of the five program areas authorized in 2005 for LETPP Homeland Security funding, information sharing between law enforcement agencies is listed first. Effective information sharing requires linking information systems for all 19,000 law enforcement agencies, not just crime data systems within UASI agencies.

As example, the "Ohio Local Law Enforcement Information Sharing Initiative," as supported by the Ohio Department of Public Safety and managed by Ohio Attorney General Jim Petro's Office and the Ohio Association of Chiefs of Police, involves the

linking of Record Management Systems (RMS) between the nearly 1,000 law enforcement agencies in Ohio. Approximately 18 percent of the Ohio law enforcement agencies are within the four Ohio UASI regions, while 82 percent of the law enforcement agencies are within Ohio's 84 SARASI counties.

The cost of linking all nearly 1,000 Ohio law enforcement agency RMS systems approximates $20–25 million. The linking of any given single agency is on, average, approximately the same, whether located in an UASI region or SARASI region. Thus, of the total cost for Ohio's Information Sharing Project, $3.5 million to $4.5 million must be allocated for UASI located agencies, while $16.5 to $20.5 million must be directed toward the law enforcement agencies in the SARASI counties (Table 4).

TABLE 4.—OHIO INFORMATION SHARING PROJECT—COST TO LINK THE 18 PERCENT OHIO UASI [15] AGENCIES AND THE 82 PERCENT OHIO SARASI [16] AGENCIES

[The proposed fiscal year 2006 LETPP budget formula will only direct up to 50 percent of the LETPP to Non-UASI or SARASI areas, while Ohio's suburban and rural SARASI agencies will need 82 percent of prevention funds to complete one aspect of prevention, i.e., information sharing between agency RMS systems]

[In millions of dollars]

	No. of counties	No. of agencies	Cost of connect agency RMSs [17]
Ohio UASIs:			
Number	4	about 175	$3.5–4.5
Percent	4.5	17	17
Ohio SARASIs:			
Number	84	about 825	$16.5–20.5
Percent	95.5	82	82
Total	88	about 1,000	$20–25

[15] UASI=Urban Area Security Initiate.
[16] SARASI=Suburban and Rural Area Security Initiative.
[17] RMS=Record Management systems.

The U.S. Department of Homeland Security's fiscal year 2006 Budget proposes the cost for information sharing prevention efforts be allocated as a 50/50 split between UASIs and SARASIs. LETPP dollars have been incorporated within the UASI and State Homeland Security Grant Programs. By approaching 2006 LETPP funding using formula percentages, States will no longer have the flexibility to allocate necessary dollars to accomplish full information sharing.

In addition, the proposed U.S. Department of Homeland Security fiscal year 2006 Budget also begins to increase the potential for funding competition between law enforcement and all other public safety first responder agencies. In the fiscal year 2004 and fiscal year 2005 budgets, Homeland Security separated the law enforcement prevention role by having the separate LETPP line item. By separating LETPP from the State Homeland Security grant programs, response issues for all First Responders (including law enforcement) were debated and explored within the funds allocated to the "State Homeland Security Grant Programs." Prevention issues did not have to be co-mingled with response discussions because LETPP existed as a separate line item.

By collapsing the LETPP program within the State Homeland Security grant program, non-law enforcement First Responders (Fire, EMA, EMS, Health) may be inclined to restrict additional funding needs of law enforcement, be they prevention or response needs, because 20 percent has already been required for law enforcement. The predictable concern will be, "Why should law enforcement get 22 or 30 or 40 percent of funding, when Congress has already assigned 20 percent of funds for police."

The proposed 20 percent formula funding of LETPP will restrict prevention efforts for the suburban and rural communities and counties, potentially increase competition between law enforcement versus all other first responders, and further inhibit police response role issues to be separated from prevention role issues.

Additionally, all suburban and rural first responders will experience reductions from the fiscal year 2005 $1.1 billion allocated to State grants. With the proposed formula allocation of $204 million incorporated within the State Homeland Security Grant Program for LETPP, State grant allocations will be reduced to $816 million (an almost $300 million reduction for SARASI or non-UASI county use for response plans, equipment and training) (Table 3). These 80 percent of First Responder and Health agencies within the SARASI communities will experience a more than 25

percent reduction from funds available for all First Responders involved in response planning, equipment and training.

In summation, we would respectfully ask that the United States Congress:

—Reinstate the Homeland Security funding category of "LETPP—Law Enforcement Terrorism Prevention Program" as a separate line item funding category;

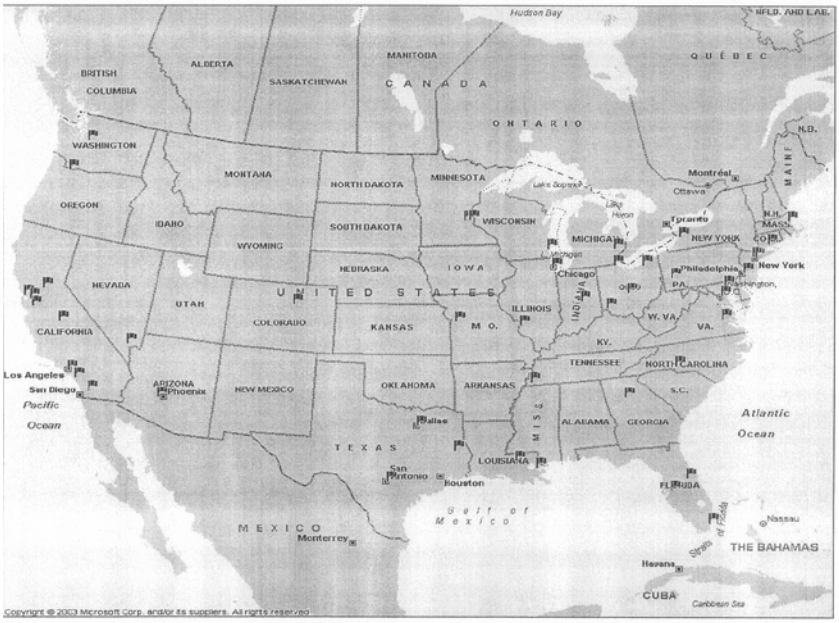
—Restrict the use of formula funding to require a threshold percentage of funding be directed toward prevention versus response efforts;

—Avoid funding allocations that will have UASI urban cities funded to the detriment of all other counties, towns and villages involved in the prevention of terrorism; and

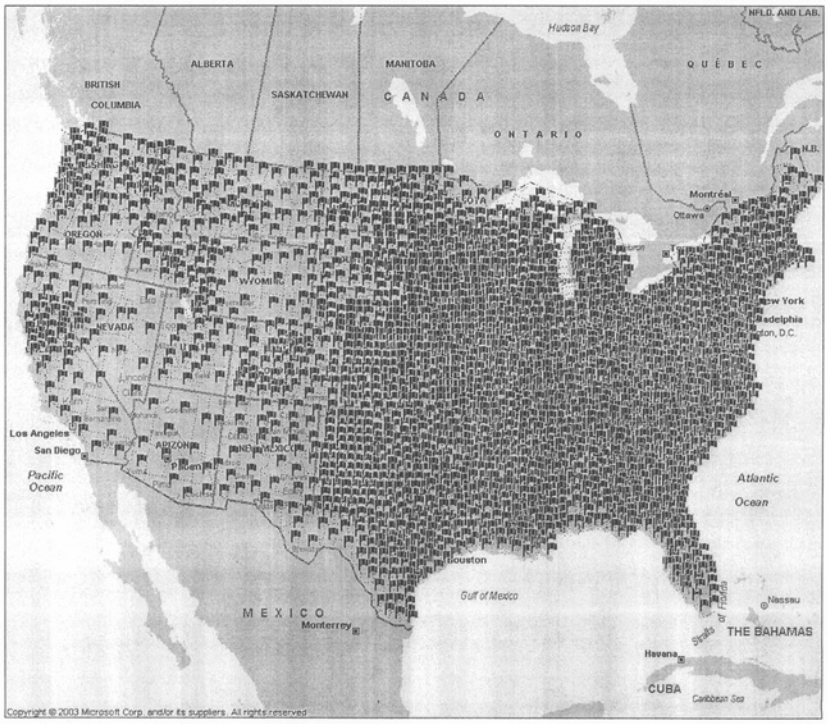
—Avoid melding the prevention plus responder roles of law enforcement into one funding category used to fund responder functions for all other first responder public safety and health agency forces.

America has not had any major terrorist incidents since 9/11. We would respectfully ask, "Why would we want to change that which is working?" Instead, would it not be more prudent to build forward, in not redesigning that which is working, but to instead address deficiencies which may have been recently identified? LETPP, as a separate line item, has served this Nation well toward accomplishing significant prevention strategies and in effectively separating out the unique prevention role 19,000 law enforcement agencies perform amongst the first responder roles all public safety forces are engaged in our 3,042 counties.

Map 1: Only 60-65 (2%) Of 3,042 U.S. Counties are UASI Counties.
However, Domestic and International Terrorists Can Plan Anywhere Within the United States.



Map 2: Of 3,042 U.S. Counties, 2,980 (98%) are SARASI Suburban and Rural Counties. Prevention, Such As Information Sharing, Involves 100% of America's Geography.



PREPARED STATEMENT OF THE UNIVERSITY OF MIAMI

Chairman Gregg, Ranking Member Byrd, and distinguished members of the Subcommittee, thank you for giving me the opportunity to provide testimony on the Disaster Resistant University initiative and to request the program be continued in the fiscal year 2006 appropriations bill of your Subcommittee.

We very much appreciate the interest Members of Congress have shown in this program. With only a small Federal investment, the Disaster Resistant University program created a model for other educational institutions to develop and implement a loss control program and created a sense of focus, pride and achievement. It is a small program with great benefits. We urge that the program be continued.

Request for Fiscal Year 2006

We respectfully request the following language in the fiscal year 2006 Department of Homeland Security Appropriations Report in the Emergency Preparedness and Response section under Predisaster Mitigation.

The Committee directs Emergency Preparedness and Response (FEMA) to continue the Disaster Resistant University Program as a separate program and to provide continued support of $500,000 directly to each of the pilot universities and $500,000 each to those selected in 2004 to implement mitigation efforts to reduce their vulnerabilities and improve protection of their students, employees, and the Federal investment in vital research.

The FEMA Disaster Resistant University (DRU) Program was created to reduce the potential for large loss of life and hundreds of millions of dollars in key Federal research and billions of dollars in damage from natural disasters. The University of California at Berkeley was the prototype and founding member of the program.

In October 2000, FEMA selected five additional universities to join Berkeley in the pilot phase of the program: the University of Alaska at Fairbanks, University of Miami, University of North Carolina at Wilmington, Tulane University, and the University of Washington at Seattle. The pilot universities have two elements in common: a vulnerability to disasters and a commitment to improve protection of students, faculty and staff, and one of our most valuable assets, intellectual property. The pilot program was funded with $700,000 in grants from predisaster mitigation funds and the U.S. Fire Administration.

Purpose of the Program

The purpose of the program is to help the Nation's colleges and universities facing the threat of natural disasters and acts of terrorism to assess their vulnerabilities and find ways to protect the lives of their students, faculty, and staff; their research; and their facilities. It will provide a framework and process for other universities to do the same.

The intent of the program is to assist universities by first providing a small grant for them to assess their vulnerabilities, devise appropriate plans, and set priorities and then to provide grants in following years of approximately $500,000 each for the universities to implement projects to reduce campus vulnerabilities to disaster.

Need for the Program

The Federal Government funds $21.1 billion annually in university research, according to the National Science Foundation statistics in 2002, the latest year available. This Federal investment in the vital intellectual property of the Nation should be protected.

In addition, universities are critical to the economic health of their surrounding communities. The ability to resume operations quickly following a disaster greatly speeds the recovery of the entire community.

Some examples of the economic impact of universities on their communities follow:

—The University of Miami is the largest private employer in Miami-Dade County with 10,157 employees and 6th largest employer overall and has an economic impact of $3.9 billion a year and 37,000 employment positions in the community.

—The University of Washington is the 3rd largest employer in the state of Washington and has a $3.4 billion impact.

—The University of North Carolina at Wilmington is the 3rd largest employer in the area and is a $400 million annual benefit to an eight county area.

—The University of California at Berkeley is the 3rd largest employer in the Bay area and generates $1.4 billion annually in the Bay area.

—Tulane University is the largest private employer in the New Orleans metropolitan area and the 5th largest private employer in Louisiana with an $842 million annual economic impact on the City of New Orleans and an annual economic impact of $1.12 billion on the state of Louisiana.

—The University of Alaska at Fairbanks is the largest civilian employer in the Tanana Valley.

In addition, many universities operate medical schools which provide essential clinical services to the residents of their communities and adjacent areas.

In the past decade, disasters have affected university and college campuses with increasing frequency. For most universities, damage that results in closure of four weeks or more would result in canceling a semester with devastating consequences for the school, the students and the community.

Many recent events underscore the need for the program: the loss of many years of research at the Texas Medical Center as result of flooding from Tropical Storm Allison; the earthquake damage to the University of California at Northridge and the University of California at Los Angeles; the facility damage and loss of life at the University of Maryland as result of a tornado; hurricane damage to the University of North Carolina at Wilmington; the earthquake damage to the University of Washington at Seattle; and the declaration by the FBI that our universities are "soft' targets for terrorists.

Status of the Program

Congress directed in the fiscal year 2003 Appropriations Bill for FEMA that $500,000 was to be available to the six existing DRUs and $100,000 each was to be available for at least six new ones to start the process. On December 31, 2003, FEMA published a Notice of Funds Availability (NOFA) for grant applications. The funds were from the PreDisaster Mitigation Fund.

Forty-four universities and four consortia applied by the March 2004 deadline. Applications were received from six Historic Black Colleges and Universities

(HBCU) and one tribal school. Applications were received from universities located in nine of the ten FEMA regions.

In October 2004 FEMA announced twenty-four colleges and universities had been selected to join the six pilots in the program. Those universities are as follows: Radford University (VA), Virginia State University, Virginia Tech, Florida Agricultural & Mechanical University, Florida International University, University System of Georgia, University of Louisville (KY), University of Mississippi, Horry-Georgetown Tech (SC), University of Memphis (TN), University of Akron (OH) Southern University (LA), University of New Orleans (LA), University of Central Oklahoma, Texas State Technical College, Texas University-Medical Center, Metropolitan Community College (MO), University of Colorado at Boulder, North Dakota State University, Sitting Bull College (ND), San Jose State University (CA), University of Southern California, University of Nevada-Reno, and the University of Oregon. These colleges and universities received Federal grants ranging from $31,000 to $100,000. The institutions are providing 25 percent of the cost.

The applications for the fiscal year 2003 funding for the pilots and the new schools had layers of requirements and were very time consuming. One of the new schools indicated that over 150 hours of staff time was required to complete the application for $100,000. However, the colleges and universities seeking to enter the program and obtain a grant put forth the effort and accepted the responsibilities of a rigorous planning and risk analysis process because of the incentive to become part of the separate DRU program and to be eligible for yearly grants of $500,000 to implement mitigation projects. In addition the colleges and universities expected to be mentored by other universities and guided by FEMA.

However, FEMA guidance for the PreDisaster Mitigation Program (PDM) issued in October 2004 for the combined 2004 and 2005 PDM grant cycles indicated that FEMA was not continuing the DRU as a separate program and recommended that colleges and universities apply for projects in the nationally competitive PDM program. Given the great benefit to FEMA and the Nation from such a small investment, this was a great disappointment to the pilots and to the new selections. Public and private nonprofit colleges and universities were already eligible applicants for the nationally competitive PDM program. Receiving a single grant for one hurricane shuttering project, one drainage improvement, or one earthquake retrofit is very helpful, but it is not a substitute for a comprehensive, multiyear program.

Given the many challenges facing our universities, it is difficult to compete for attention and money for disaster preparedness and mitigation when there is not an immediate threat. However, designation as a Disaster Resistant University has real value. The pilot universities found that the designation as a Disaster Resistant University and the expectation of continuing to participate in the program brought attention and commitment at the highest levels of the universities. The networking and partnerships built with Federal, State, and local emergency management officials and other entities serving the public, such as hospitals and utilities, have benefits to the communities far beyond the scope of the original program and certainly way beyond the amount of the grants. Participating in the program created a framework for disaster planning and mitigation activities that helped universities focus and enhance efforts to protect their students, faculty, staff, vital research, and facilities. Two of the great values of the program which should not be overlooked have been the mentoring and exchanging of ideas among participating universities and the pilots spreading the FEMA mitigation message as they share their experiences at many different national and regional meetings of educational institutions.

We again thank you for the opportunity to provide written comments and respectfully urge that the DRU program be continued. A summary of previous Congressional interest in this program is attached. We would welcome the opportunity to provide additional information or to discuss the program further with your staff.

Summary of Congressional Interest

We very much appreciate the support Congress has given this program.

Fiscal Year 2002

The Conference Report on the VA, HUD and Independent Agencies Appropriations bill for 2002 (House Report 107–272) contained the following language:

The conferees believe that many of the Nation's universities are vulnerable to disaster and urge FEMA to continue its Disaster Resistant University program and expand the scope to include safe-guarding university assets from acts of terrorism.

Fiscal Year 2003

The Conference Report on the fiscal year 2003 Omnibus bill in the FEMA section of the VA, HUD and Independent Agencies stated the following:

The conferees are in agreement that FEMA should continue the Disaster Resistant University program and direct FEMA to carry out the direction contained in House Report 107–740.

House Report 107–740 stated the following:

Finally, the Committee notes that in September of 2000 FEMA selected five universities to join the University of California at Berkeley in the pilot phase of the Disaster Resistant University program: University of Alaska/Fairbanks, University of Miami, University of North Carolina/Wilmington, Tulane University, and University of Washington/Seattle. The purpose of the program is to help the Nation's colleges and universities facing the threat of natural disasters to assess their vulnerabilities and find ways to protect their research, facilities and the lives of students, faculty and staff. The Committee directs FEMA to continue the Disaster Resistant University Program with grants of $500,000 to each of the six pilot Disaster Resistant Universities and $100,000 each to at least six additional universities, including at least one HBCU, to join the program.

Fiscal Year 2004

The Senate Report on the Department of Homeland Security Appropriations bill (S. Report 108–86) included the following language under the National Pre-Disaster Mitigation Fund which was funded at $150,000,000.

The Committee encourages the Department to continue the existing Disaster Resistant University program at the fiscal year 2003 level.

The House receded to the Senate in the conference agreement.

PREPARED STATEMENT OF THE UPPER MISSISSIPPI RIVER BASIN ASSOCIATION

The Upper Mississippi River Basin Association (UMRBA) is the organization created in 1981 by the Governors of Illinois, Iowa, Minnesota, Missouri, and Wisconsin to serve as a forum for coordinating the five States' river-related programs and policies and for collaborating with Federal agencies on regional water resource issues. As such, the UMRBA has an interest in the budgets for the U.S. Coast Guard and the Federal Emergency Management Agency (FEMA).

Both the Coast Guard and the FEMA have vital functions specifically related to homeland security that must be adequately funded. But both also have other traditional missions that are equally important to public health and safety, economic well-being, and environmental protection. For the Coast Guard, these include activities such as aids to navigation, vessel and facility inspections, emergency response, and mariner licensing. For FEMA, key traditional missions include the National Flood Insurance Program, flood map modernization, hazard mitigation, and response to floods and other natural disasters. Nowhere are these services more important than on the Upper Mississippi River System, which supports a vital link in the inland waterway transportation system, some of the Nation's most productive agricultural land, population centers ranging from small towns to major metropolitan areas, and a nationally significant ecosystem.

COAST GUARD OPERATING EXPENSES

A continuing priority for the UMRBA is the Coast Guard's Operating Expenses account. The President's fiscal year 2006 budget proposal includes $5.55 billion for this account, an increase of almost 8 percent from the fiscal year 2005 enacted level. However, this net increase of $390 million for Operating Expenses will be largely consumed by specific increases tied to implementation of the Maritime Transportation Security Act (MTSA); increased personnel costs; and operating costs for new vessels, aircraft, and facilities related to the Coast Guard's saltwater responsibilities. These initiatives are important in their own right and will benefit a range of Coast Guard missions. However, it is also true that the Coast Guard's non-security missions on the Nation's inland waterways will be under continued strain as the inflation-adjusted resources for many of these missions remain static or shrink.

When the Department of Homeland Security was formed, the UMRBA strongly supported the Coast Guard's stated objective of sustaining traditional missions near their pre-9/11 levels. These traditional missions are critical to the safe, efficient operation of the Upper Mississippi River and the rest of the inland river system. Under these mission areas, the Coast Guard maintains navigation channel markers, regulates a wide range of commercial vessels in the interest of crew and public safety, and responds to spills and other incidents. The beneficiaries include not only commercial vessel operators, but also recreational boaters; farmers and others who ship materials by barge; and the region's citizens, who benefit enormously from the river as a nationally significant economic and environmental resource.

Even prior to September 11, recent years had brought a number of changes to the way the Coast Guard operates on the inland river system, including elimination of the Second District; closure of the Director of Western Rivers Office; decommissioning the Sumac, which was the largest buoy tender on the Upper Mississippi River; and staff reductions. While the States understand the need for efficiency, the cumulative impacts of these changes must be carefully monitored, particularly in light of the increased demands that we are now placing on the personnel and assets that remain in the region. The UMRBA is quite concerned that staff reductions and resource constraints have combined to impair the Coast Guard's ability to serve as an effective, proactive partner.

Specifically, increased security demands have reduced the staff assigned to vessel inspections and limited the Coast Guard's investigation of reported spills. Sending a single person to conduct vessel inspections reduces the rigor of those inspections, and, in a worst case scenario, potentially puts the inspector at risk. Similarly, electing not to respond to reports of small spills means some of these spills will go uninvestigated and puts increased demands on local officials, who do not have the Coast Guard's expertise or resources. Moreover, it could result in costly delays should a spill turn out to be larger than first reported, an all-too-common occurrence. Temporary adjustments initially made to accommodate immediate security needs are now evolving into long term standard operating procedures. While everyone recognizes the need to adjust to our new security environment, it is essential for the Coast Guard to retain the capacity to perform its traditional missions on the Upper Mississippi River. Toward that end, the UMRBA supports the President's fiscal year 2006 budget request for the Coast Guard's Operating Expenses account, and urges Congress to ensure that sufficient resources from within this account are allocated to the Coast Guard's inland river work.

Research, Development, Testing, and Evaluation

Through its Research, Development, Testing, and Evaluation (RDT&E) program, the Coast Guard conducts cutting edge research in several critical areas, including oil spill prevention and response, risk assessment, and mariner safety. Of particular note, researchers at the Coast Guard's Groton, Connecticut Research and Development Center have made invaluable contributions to State-of-the-art fast water spill response, in situ burning, and human error reduction. However, the President is once again proposing to shift the Coast Guard's RDT&E funding to the Department of Homeland Security's Science and Technology (S&T) Directorate. This proposal represents precisely the kind of diminution of the Coast Guard's non-security missions with which the UMRBA and others have repeatedly expressed concern. Research on innovative oil spill recovery equipment or new methods for combating crew fatigue will likely be lost in the department-wide S&T Directorate, with its overwhelming focus on homeland security issues. Moreover, the President's proposal appears to be inconsistent with Section 888 of the Homeland Security Act, which calls for "the authorities, functions, and capabilities of the Coast Guard to perform its missions . . . [to] be maintained intact." The UMRBA urges Congress to provide adequate and direct funding of approximately $24 million to the Coast Guard's multi-mission RDT&E program in fiscal year 2006. This is the amount the Administration suggests the Coast Guard would receive from the S&T Directorate's competitive funds in fiscal year 2006, and is a $5.5 million increase over the fiscal year 2005 RDT&E appropriation.

Reserve Training

The President is requesting $119 million for Coast Guard Reserve Training in fiscal year 2006, an increase of $6 million, or 5 percent, over the fiscal year 2005 enacted level. The UMRBA States are keenly aware of the importance of the reserve forces. During major flood events on the inland rivers, reservists have consistently provided exemplary service, augmenting the Coast Guard's capabilities and helping to protect public health and safety. More recently, many reservists have been called to active duty, enabling the Coast Guard to meet many new security-related demands. On the inland rivers, this has included increased patrols near critical facilities and development of security plans for key inland ports. The UMRBA urges Congress to fund Reserve Training at $119 million in fiscal year 2006, thereby helping to maintain a Coast Guard reserve that can effectively execute both homeland security- and natural disaster-related missions.

Boating Safety Grants

The Coast Guard's boating safety grants to the States have a proven record of success. The Upper Mississippi is a river where all types of recreational craft routinely operate in the vicinity of 15-barge tows, making boating safety all the more impor-

tant. As levels of both recreational and commercial traffic continue to grow, so too does the potential for user conflicts.

Boat safety training and law enforcement are key elements of prevention. However, the future of this successful grants program is uncertain. Following the pattern of recent years, the President has requested $59 million in fiscal year 2006 funding for boating safety grants to the States. This is the amount historically authorized without annual appropriation from the Boat Safety Account, which is funded by a tax on fuel for recreational motor boats. Successive Administrations have not typically exercised their option to request an additional $13 million in annual appropriations for the grants. However, the authority for the funding from the Boat Safety Account must be extended if the program is to continue in fiscal year 2006. Such a provision is currently being considered as part of pending transportation legislation. The UMRBA urges prompt reauthorization of the Boating Safety Program, and funding of this important work at $72 million annually.

FEDERAL EMERGENCY MANAGEMENT AGENCY (EMERGENCY PREPAREDNESS AND RESPONSE DIRECTORATE)

Hazard Mitigation

UMRBA is particularly interested in FEMA programs that help mitigate future flood hazards. Mitigation, which is the ongoing effort to reduce or eliminate the impact of disasters like floods, can include measures such as relocating homes or community facilities off the floodplain, elevating structures, and practicing sound land use planning. Mitigation planning and projects are essential to reducing the Nation's future disaster assistance costs. Given the importance of mitigation, UMRBA supports the Pre-Disaster Mitigation (PDM) grant program, which was created in fiscal year 2003 and for which the President is requesting $150 million in fiscal year 2006. While the PDM grant program is still relatively new, it holds promise for enhancing communities' ability to prevent future damages, particularly in areas that have not experienced a major disaster and thus have not had access to post-disaster mitigation assistance through the Disaster Relief Fund. In addition, pre-disaster mitigation assistance is an effective means of meeting the ongoing need in all communities to plan for future floods and reduce their vulnerability before the next flood disaster.

In fiscal year 2003, forty communities in the five Upper Mississippi River Basin States received PDM competitive grants, totaling $3.4 million. While most were relatively small planning grants, funding was also provided for acquisitions, safe rooms, and electric utility protection. The application period for the second round of grants (fiscal year 2004–2005 combined) just ended. While there have been concerns expressed about the complexities of the competitive process, there is no doubt that communities need such grants to help them develop effective mitigation plans and reduce the impacts of floods. Thus UMRBA supports the President's fiscal year 2006 funding request of $150 million for the PDM program.

Flood Map Modernization

Flood maps are not only used to determine risk-based National Flood Insurance Program premium rates, but also provide the basis for local regulation of flood hazard areas and for State and local disaster response planning. However, current flood maps are rapidly becoming obsolete due to the effects of land use changes in the watersheds. When outdated maps underestimate flood depths, it can often lead to floodplain development in high risk areas. It is therefore important that flood maps be updated on an ongoing basis and in a timely way.

The President's fiscal year 2006 budget proposes $200 million for FEMA's Flood Map Modernization program. While funding for flood maps has increased substantially since the Map Modernization initiative began in fiscal year 2003, there are growing concerns about the adequacy of the original time and cost estimates. For instance, producing updated and accurate maps often requires that new studies be conducted. However, the existing map modernization budget is only sufficient to fund actual mapping costs and will not adequately cover the costs of necessary associated tasks, such as new flood elevation studies or levee certifications. Given that mapping needs are being prioritized based on population, rather than flood risk or need, it is not clear when relatively sparsely populated counties along the Mississippi River will be mapped. Ironically, the Federal Government, through the U.S. Army Corps of Engineers, recently spent approximately $17 million to develop new flood profiles for the Upper Mississippi and Lower Missouri Rivers. Unfortunately this updated information cannot be fully utilized until sufficient funding is made available to modernize and digitize the flood maps for river communities. Thus, the UMRBA urges Congress to provide adequate funding for map modernization, includ-

ing sufficient funding to develop new maps for the Upper Mississippi and Lower Missouri Rivers based on the new flood profiles.

LIST OF WITNESSES, COMMUNICATIONS, AND PREPARED STATEMENTS

Page

Aguirre, Eduardo, Jr., Director, U.S. Citizenship and Immigration Services, Department of Homeland Security 1
Prepared Statement of 32
Statement of 30
Albright, Dr. Penrose C., Assistant Secretary for Science and Technology, Department of Homeland Security 349
Prepared Statement of 353
Questions Submitted to 400
Statements of 351
Allard, Senator Wayne, U.S. Senator From Colorado, Statement of 147
American Public Transportation Association, Prepared Statement of 435
Association of State Floodplain Managers, Inc., Prepared Statement of 439

Bonner, Robert C., Commissioner, Customs and Border Protection, Department of Homeland Security 1
Prepared Statement of 18
Statement of 15
Byrd, Senator Robert C., U.S. Senator From West Virginia:
Letter From 5
Questions Submitted by 99, 229, 416, 429
Statements of 3, 136, 350

Chertoff, Michael, Secretary, Department of Homeland Security 117
Prepared Statement of 121
Statements of 120
City of San Marcos, Texas, Prepared Statement of 442
Clerici, John M., Esq., Partner, McKenna, Long & Aldridge, LLP 388
Prepared Statement of 391
Statement of 388
Coalition of Northeastern Governors, Prepared Statement of 443
Cochran, Senator Thad, U.S. Senator From Mississippi:
Prepared Statement of 155
Questions Submitted by 48, 218
Statements of 1, 359
Craig, Senator Larry, U.S. Senator From Idaho, Statement of 140

Domenici, Senator Pete V., U.S. Senator From New Mexico:
Questions Submitted by 90, 221, 413
Statement of 151

Feinstein, Senator Dianne, U.S. Senator From California, Statement of 138
Franz, Dr. David, Chief Biological Scientist, The Midwest Research Institute 376
Prepared Statement of 378

Garcia, Michael J., Assistant Secretary, Immigration and Customs Enforcement, Department of Homeland Security 1
Prepared Statement of 10
Statement of 8
Greater Orlando Aviation Authority, Prepared Statement of 443
Gregg, Senator Judd, U.S. Senator From New Hampshire:
Opening Statements of 117, 349
Questions Submitted by 163, 400, 421

Page

Inouye, Senator Daniel K., U.S. Senator From Hawaii, Questions Submitted by 111
International Association of Emergency Managers, Prepared Statement of 445

Kohl, Senator Herb, U.S. Senator From Wisconsin, Statement of 153

Leahy, Senator Patrick J., U.S. Senator From Vermont:
Questions Submitted by..... 113, 341
Statement of 2

Murray, Senator Patty, U.S. Senator From Washington:
Prepared Statement of 145
Questions Submitted by 344
Statement of 142

National:
Emergency Management Association, Prepared Statement of 447
Flood Determination Association, Prepared Statement of 452

Ohio Department of Chiefs of Police, Inc., Prepared Statement of 453

Read, J. Leighton, M.D., General Partner, Alloy Ventures 382
Prepared Statement of 386

Sarnoff Corporation, Prepared Statement of 396
Shelby, Senator Richard C., U.S. Senator From Alabama, Questions Submitted by 91
Simonson, Stewart, J.D., Assistant Secretary, Office of Public Health Emergency Preparedness, U.S. Department of Health and Human Services 359
Prepared Statement of 361
Questions Submitted to 421
Specter, Senator Arlen, U.S. Senator From Pennsylvania, Questions Submitted by 428
Stevens, Senator Ted, U.S. Senator From Alaska, Questions Submitted by..... 89, 219

University of Miami, Prepared Statement of 459
Upper Mississippi River Basin Association, Prepared Statement of 462

SUBJECT INDEX

DEPARTMENT OF HOMELAND SECURITY

Page

Absconders and Violators of Release Orders and Return Orders 150
Accomplishments in Biodefense 351
Additional Committee Questions 48, 162, 400
Advance Appropriation 372
Agricultural Inspections 169
Air:
  And Marine Operations—Recapitalization 75
  Cargo 285
    Security 175
  Carrier Fees 288
  Traveler Satisfaction 188
Airborne Rapid Imaging for Emergency Support 326
Airport Security 148
All:
  Hazards 313
  State Minumum 342
Alternatives to Detention 35
America's Shield Initiative 72, 105
AMO Fleet Modernization Plan 274
Anthrax 360
Antidumping/Countervailing Duty Collections 37
APHIS—Food Safety Inspectors 274
Arizona Border Control Initiative 67
Assessments and Evaluations 337
Asylum and Expedited Removal 68
Attrition Rate 310
Automated:
  Commercial Environment 74
  Identification System 305
Automation/Information Technology 26
Aviation Security 156, 218
Avoiding Future Fund Lapses 231
Background on GSA Basic Purchasing Agreement With IMC 135
Backlog:
  Elimination 31
  Reduction Plan 81
Backscatter Technology 154
Base Decreases 289
Best Practices 326
Biodefense 353
Biological or Chemical Attack 350
Bioshield 349
Bioterrorism and Cooperative Efforts 373
BioWatch:
  Detection 417
  Response 417
Border:
  Needs:
    Security Updgrades at Ports 221
    UAV Technology 221
  Patrol 110, 138, 343
    Agent Staffing Increases 40

Page

Border—Continued
Patrol—Continued
Aircraft Replacement 47
Apprehensions 109
Checkpoints 114
Stationing of Agents 110
Vehicles 98
Personnel:
Manpower 222
Training at FLETC 222
Problems 141
Security 95, 271
Budget:
Amendment 137
Issues 9
Request 367
For Fiscal Year 2006 13
Shortfalls and Increased Staffing for the Border Patrol 2
Buffer Zone Protection Plans 335
C–130Js 308
C–TPAT 278
Call Centers 89
Cargo:
Container Security 271
Security 144, 344
Supply Chain Security 18
CBP Response 7
Cell Technology Versus Culture Technology 371
Cerro Grande Fire Claims 329
Challenges 12
Chemical:
And Biological:
Agents 366
Detection Program 413
Countermeasures 420
Detectors 367, 416
Security 333
Chief Information Officer 260
CIS Local Ombudsman 100
Citizens Corp 326
Citizenship and Immigration Services Funding 115
Classified vs. Sensitive Information 231
Coast Guard:
C–130 211
Support of NSF Research Operations in the Polar Regions 306
Collection of:
Antidumping and Countervailing Duties 279
Duties 106
Communication:
And Technology Systems 213
With ICE Employees 9
Comprehensive:
Border Control Strategy 17
Review of the Department 163
Concerns of Employees 257
Consulting With Congress 262
Container Security 105
Initiative: Expansion and Regularization 103
Continued Funding Shortfalls—ICE 48
Contract Employees 337
Contracting Out Report 232
Covert Surveillance Aircraft 305
Creating a 21st Century Department 132
Critical Infrastructure Protection 199
Cross-Cutting Functions and Integration 122
Customer Service 82
Customs:
And Border Protection—The Second Year 19

Page

Customs—Continued
Trade Partnership Against Terrorism 72
Cyber Crimes 284
Debt Management Center 114
Deepwater 209
Budget 295
Program Management 298
Default of a Surety Company 39
Demonstration of Ideas by People 372
Department of Homeland Security:
And BioShield 401
BioWatch, and Detection of Events 404
"Branding" Not Completed 277
Headquarters 231
Intelligence .....
Mission 198
Role 158
Reports Due 260
Role in Detection Equipment 405
Departmental Reorganization 166
Detailees to the:
Department 235
White House 233
Detention:
And Removal 10
Bedspace 101
Facilities 282
Domestic Nuclear Detection Office 192, 418
Drug Trafficking 229
Electronic Surveillance 135
Along the Border 119
Emergency Response Fund 311
Emerging:
Checkpoint Explosives Technology 292
Issues 156
EMS First Responder Funding 317
Expedited:
Removal 150
Traveler Expanding Overseas 269
F2B Preference Visa Petition 112
Federal:
Air Marshals 78
Service 10
Law Enforcement Training Center (FLETC) 216
Protective Service 80
FEMA Personnel 330
Financial and Procurement Controls 208
FIRE Grant Funding 314
First Responders (General) 343
Fiscal Year:
2004 Workload Statistics 16
2005 Accomplishments 125
2006 Budget Request 9, 30, 119, 128
Enhancements 13
For Citizenship and Immigration Services 3
Fisheries Enforcement 219
Flood Map Modernization 328
Foreign:
And Domestic Repair Station Inspections 294
Student Visas 154
Fugitive Operations 78
Funding:
For First Responders 172
Issue 4
Global Supply Chain Security 169
H2B Visa Program 3
Hammer Training 345
Hazard Mitigation 327

Page
Hazardous Materials Endorsement for Commerical Driver's License 293
Health and Human Services and BioShield 421
Hearings on the PATRIOT Act 261
HH–65 Helicopter Re-engining 211
Hiring Journalists 249
Homeland Secure Data Network 166
Human:
Resources 207
Smuggling 81
I–91 Checkpoint 41
I-Staff 206
IA's Role in Intelligence Community 331
IAIP:
Coordination of Protection 202
Hiring Difficulities 200
ICE:
CBP Merger 344
Cyber Crime Center 89
Hiring in Fiscal Year 2006 39
Response 7
IDENT/IAFIS 272
Integration 273
Update 106
Illegal Immigrants..... 92, 279
Immigration 118
Advisory Program 71
And Customs Enforcement 341
Enforcement 101
Officers in Local USCIS Offices 111
Services 89
Impact of:
Bush Amnesty on Backlog Reduction/Workload 99
ICE Budget Shortfall 102
Late Duty Collection on Crawfish Industry 104
Networking 152
REAL ID on Backlog Reduction/Workload 271
Implementation of the Visa Reform Act 45
Imported Shrimp Industry 98
Improvement in Customer Service 31
Improving:
Airport Security 154
National Preparedness and Response 130
Indemnification 399
Independent Review of Collective Bargaining Disputes 257
Information Concerning the PATRIOT Act 261
Initial Preliminary Orders in Liquidation 39
Institutional Removal Program 79
Integration of CBP Air and Marine Assets 47
Intelligence 118
Reform:
Act/Border Patrol Staff Increases 44
And Terrorism Prevention Act 4
Bill Authorizations 249
International Partnerships 163
Interoperability:
Communications 315
Standards 315
Interoperable Communications 174
Introduction:
And Overview 18
Of Diseases From Other Countries 374
Investigations:
And Intelligence 10
Of Arms Export Control Act Violations 102
IT issues 118
L1 Visa Inter-Agency Task Force 45
Lack of:
BioShield Funding for RAD/NUC Response 429

Page

Lack of—Continued
Funding for Border Security 270
Land Port of Entry 90
Law Enforcement Support Center 2, 114
Legal Orientation Programs 115
Leveraging Technology 131
LIFE Act 111
Lobbying Rules 229
Management and:
Administration 336
Staffing 165
Mandatory Termination With No Outside Review 258
Maritime:
Security Cutter—Large Operational Costs 309
Transportation Security Act Implementation 299
Measures for Determining Budgets 284
Meeting:
Our Twin Goals: Building More Secure and More Efficient Borders 21
With Unions 261
Merging CBP and ICE 272
Merit System Protection Board (MSPB) 257
Movement of Resources 157
NAC 208
National:
Bio and Agrodefense Facility 420
Border Security Assessment 101
Center for Critical Information Processing and Storage 219
Preparedness Goal 170
Response Planning 311
Security Mission 31
Need for Additional Assistance From the Subcommittee 162
New:
Mexico Capabilities—Training at Playas 222
Office of Screening Coordination and Operations 41
Products to Protect Against Bioterrorism Acts 368
NOAA Weather Radios 340
Non-Profit Grant Funding 316
NonGovernmental Screening Group 372
Northern Border:
Air Wing 346
Prosecutions 346
Security 346
Number of Border Patrol Agents Needed 133
Observations Regarding the Department of Homeland Security 151
Office of:
Citizenship 84
Fraud Detection and National Security 82
Screening Coordination and Operations 167
Mission 44
(9/11 Commission Recommendation) 65
Security 204
One Face at the Border 16
1–800 Customer Service Numbers 112
Operation Predator 91
Other:
Concerns 119
Traditional Missions 27
Overhead Cost Sharing 78
Overtime:
Pay While Receiving Training 104
Rate 310
Overview of ICE Fiscal Year 2006 Budget Request 10
Passenger Air Fees 285
Passport Privacy 271
Pay:
For Performance 259
Increase 310
Personnel Concerns 119

Page
Port Security 143, 344
Assessments 304
Estimates 304
Grant:
Coordination 317
Program 304
Port/Rail/Transit 313
Ports of Entry in Vermont 113
Pre-Disaster Mitigation Grants 330
Pre-Packaged News 286
Preparation for Biological Attack 160
Private:
Screeners 293
Sector Interest in BioShield 430
Progress Since March 2003 30
Protecting Americans 361
Pulsed Fast Neutron Analysis 276
R&D Consolidation 191
Radiological/Nuclear Countermeasures Test and Evaluation Complex 419
Rapid Prototyping 411
Recruiting 308
Regions Initiative 205
Registered Traveler 295
Repatriation Program With Mexicans 150
Requirements Gap 300
Research and:
Development 213, 310
Technology:
Domestic Nuclear Detection Office (DNDO) 228
Generally 225
NISAC 227
Review of ICE Accomplishments 11
Revolutionizing the Borders 128
Risk:
Based Approach 125
Of Liability 399
Role of Science and Technology Directorate 194
Rudeness of Customs Employees 148
S&T:
Directorate's Interagency Collaboration 352
University Partnership Program 197
SAFETY Act 409
Satisfaction With Status Quo Budget 150
Science & Technology Directorate and:
Integrated Biosurveillance 401
Standards 407
Screening Workforce Performance 287
SeaTac Airport 347
Second Stage Review 122
Section 605 of Vision 100 288
Secure:
Electronic Network for Travelers Rapid Inspection Program (SENTRI) 71
Flight 262
And Privacy 264
Movement to SCO 264
Security and Prosperity Partnership of North America 259
Shelf Sensitive Vaccines 370
Significant ICE Achievements 8
SIPRINET 309
Six-Month Average for Processing Benefits Applications 37
Slow Pace of Grant Distributions 312
Southwest Border Control 139
Stabilization of Senior Management 161
Staffing 85, 282
Model 60
Status of:
Security of the United States 2 Years After the Establishment of the Department of Homeland Security 6

Page

Status of—Continued
Technology in Use on the Borders and Detention Space 134
Status Quo Budget Request 149
Stepped up Enforcement Along the Border 142
Strategic:
Approach to Addressing Medical Countermeasure Gaps 362
National Stockpile Today 362
Strengthening Law Enforcement 129
Supply Chain and Container Security 271
System:
That Monitor Supply of Pharmaceutical Products 369
Weaknesses 365
Tasking the FLRA and MSPB 258
Technology Transfer 317
Temporary Worker Program 142
And Backlog Elimination Program 97
Terrorist Travel (9/11 Commission Report) 65
Thefts of Luggage of Passengers 158
Threats in Order of Priority 397
TOPOFF Exercise 161
Trade/Travel Facilitation 17
Training of:
Border Patrol Agents 134
CBP Inspectors 108
Supervisors 258
Transportation of Butant Stoves (Without Butane) on Airplanes 219
TSA 118, 156
Air Carrier Security Fees 178
Contract Screeners 179
"No Fly" Lists/Secure Flight 185
Passenger Fees 177
R&D 295
Screener Training 182
Spending Abuses 287
TWIC Program—Why the Delay? 269
UAVs 220
Unfair Trade Practices—Catfish Imports 46
University Centers of Excellence 419
US VISIT 168, 268
When Will We Have a Real "Exit" Component? 267
USCIS Response 7
Use of:
IDENT, IAFIS and US VISIT 159
Radiation Monitors 36
Stolen Passports—Inspector General Report 68
Unmanned Aerial Vehicles 276
Vehicle Fleet Management Report 274
Vetted Traveler Programs 42
Violating the DHS Appropriations Act 341
Visa:
Overstays 92
Security Unit 76
Waiver 139
Program: Further Extension 99
Visit to One of the Ports 148
War on Drugs—Historical 111
Weapons of Mass Destruction Detection Technology 17
White House Mail 310
Worksite Enforcement 75, 284

○