S. Hrg. 108–332

NOMINATION OF ADMIRAL JAMES M. LOY

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

ON THE

NOMINATION OF ADMIRAL JAMES M. LOY TO BE DEPUTY SECRETARY OF HOMELAND SECURITY

NOVEMBER 18, 2003

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

91–044 PDF WASHINGTON : 2004

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 GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
ARLEN SPECTER, Pennsylvania
ROBERT F. BENNETT, Utah
PETER G. FITZGERALD, Illinois
JOHN E. SUNUNU, New Hampshire
RICHARD C. SHELBY, Alabama

JOSEPH I. LIEBERMAN, Connecticut
CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
RICHARD J. DURBIN, Illinois
THOMAS R. CARPER, Deleware
MARK DAYTON, Minnesota
FRANK LAUTENBERG, New Jersey
MARK PRYOR, Arkansas

MICHAEL D. BOPP, *Staff Director and Chief Counsel*
JOHANNA L. HARDY, *Senior Counsel*
TIM RADUCHA-GRACE, *Professional Staff Member*
JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Counsel*
HOLLY A. IDELSON, *Minority Counsel*
JENNIFER E. HAMILTON, *Minority Research Assistant*
AMY B. NEWHOUSE, *Chief Clerk*

CONTENTS

	Page
Opening statements:	
Senator Collins	1
Senator Stevens	3
Senator Akaka	5
Senator Carper	6
Senator Lautenberg	7
Prepared statement:	
Senator Durbin	25

WITNESSES

TUESDAY, NOVEMBER 18, 2003

Hon. Daniel K. Inouye, a U.S. Senator from the State of Hawaii	4
Admiral James M. Loy to be Deputy Secretary of Homeland Security	9

ALPHABETICAL LIST OF WITNESSES

Inouye, Hon. Daniel K.:	
Testimony	4
Prepared statement	25
Loy, Admiral James M.:	
Testimony	9
Prepared statement	27
Biographical and professional information requested of nominees	30
Pre-hearing questionnaire and responses for the Record	39
Post-hearing questions and responses for the Record from:	
Senator Collins	162
Senator Lieberman	181
Senator Durbin	184
Senator Lautenberg	186
Senator Specter	193

APPENDIX

Letter from Admiral Loy, dated Feb. 23, 2004, with a correction for a factual error contained in response to pre-hearing question No. 63	194

NOMINATION OF ADMIRAL JAMES M. LOY

TUESDAY, NOVEMBER 18, 2003

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 2:32 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Stevens, Akaka, Carper, and Lautenberg.

OPENING STATEMENT OF SENATOR COLLINS

Chairman COLLINS. The Committee will come to order. Today the Committee on Governmental Affairs will consider the nomination of Admiral James Loy to be the Deputy Secretary of the Department of Homeland Security, the No. 2 post in this important Department.

We are fast approaching the first anniversary of the Homeland Security Act which established the new Department. Integrating 22 Federal agencies was necessary to enhance the security of the United States and the safety of its people in this environment of global terrorism. But unifying 22 agencies and more than 170,000 employees is an extraordinary challenge. Secretary Ridge and his team are to be commended for their tireless efforts on what is a monumental undertaking.

But there is a seat at the helm that is now empty and I can think of no finer person to fill it than the nominee who is before us today. Admiral Loy, you have spent 40 years on the front lines of homeland security. In 1998, during your Commerce Committee hearing to be the commandant of the Coast Guard, Senator Inouye remarked, "you are to be commended for the decades of superb service you have given to your country. You have gotten this nomination the old-fashioned way—you have earned it." You have certainly earned this one, too.

Helping to run this enormous new Department will take all of your skills, dedication, and savvy. The Department of Homeland Security has to address an endless number of threats and issues each and every day, yet it must be able to balance security concerns with the need to preserve our American way of life.

My home State of Maine shares more than 600 miles of border with Canada making border security issues especially important to me. The people, communities, and businesses on both sides of the border depend upon each other for friendship, mutual aid, and economic success. Many families, including my own, have relatives on

both sides of the border and the ease of crossing has allowed them in the past to maintain strong family ties. I understand and certainly support the efforts that the United States is making to improve border security at home, but as the Department moves forward on policies that tighten border security it must also take into consideration the social and economic ramifications of any changes.

Admiral Loy, should you be confirmed, as I believe you will be, the Committee will also support your efforts to improve the level of preparedness in every community. This Committee has held hearings and approved legislation to strengthen homeland security grant programs, to put cutting edge counterterrorism technologies in the hands of local law enforcement, and to strengthen American seaports against a terrorist attack. We must make certain that our communities receive a long-term, steady stream of funding to prevent a future terrorist attack and to respond should the worst occur.

The Committee has already approved legislation that I introduced that provides a solid baseline of funding to each State but that allocates the majority of the funding, more than 60 percent, to States based on the individual circumstances of risk, threat, and vulnerability. We hope that you will work with the Committee to ensure that this legislation is enacted into law next year.

I also appreciate your efforts to improve coordination within the Department and with other agencies. The Department's efforts to set up a single website for many homeland security grant programs is a step in the right direction. In addition, however, we need to reduce paperwork, standardize equipment and training standards, and coordinate emergency preparedness plans. If confirmed, I hope that you will work with this Committee to forge a bipartisan consensus on all of these issues, and I trust that you will let us know promptly if you need more tools or resources to help our States, communities, and first responders.

Finally, let me comment on your outstanding 38-year career in the Coast Guard. When the new Department of Homeland Security was first being debated Senator Stevens and I joined forces to ensure that the Coast Guard's vital traditional missions, such as search and rescue, were not compromised as the Coast Guard took on additional homeland security responsibilities. I am confident that given your long career in the Coast Guard you will ensure that both the letter and the spirit of the Stevens-Collins amendment are followed.

Perfect timing; the Senator from Alaska has come in.

In short, we are very pleased to have you here today and I look forward to hearing the introduction of you, the formal introduction by two of our most esteemed colleagues. I would first call upon the—now you are each pointing at the other.

Senator STEVENS. He is senior.

Chairman COLLINS. I will call on the distinguished senior Senator from Hawaii. I want to tell you that I had a big debate with my staff over whom I should call upon first, the President pro tempore or the senior member, and it was a toss-up. So since Senator Stevens has suggested I proceed with the distinguished Senator from Hawaii, I am going to follow his advice, which is always sound. Senator Inouye.

Senator INOUYE. Madam Chairman, I very seldom disagree with my brother but he is the President pro tempore, and most importantly, this day is his birthday.

Chairman COLLINS. That is true and we hope to celebrate that later today.

Senator INOUYE. If you want this nomination to go through, you had better get the octogenarian—— [Laughter.]

Chairman COLLINS. Senator Stevens, I think the distinguished Senator has yielded to you.

Senator STEVENS. Thank you very much, Madam Chairman.

Chairman COLLINS. We welcome you.

OPENING STATEMENT OF SENATOR STEVENS

Senator STEVENS. It is a privilege to be here with you and to introduce Admiral Loy to our Committee. He has had a long and distinguished record of public service. You may have already stated this, his career spans over 30 years with the Coast Guard. He graduated from the Coast Guard Academy in 1964 and came through the ranks to be the commandant in May 1998.

Now my State has a unique relationship with the Coast Guard. We have more than half the coastline of the United States, 6,640 miles of coastline. That literally makes us stewards of the coastline longer than all 48 States combined. We have the Coast Guard's largest base on Kodiak Island. I had some experience with that when I was a brand new Senator. Senator Nixon wanted to close the Kodiak Naval Station and we thought it was a place that should have some presence. I went to the Coast Guard and asked them to come visit Kodiak and was able to convince them to move a small station there. They have since learned that that is the place from which we can guard the Pacific and all its resources for the United States.

I got to know Admiral Loy well when he served as commandant. During his tenure he led the Coast Guard's effort to rebuild and restore readiness, he rebuilt the Coast Guard's workforce to authorized levels, improved retention and prepared the Coast Guard to fulfill its future duties and responsibilities. He also made sure the Coast Guard had the resources it needed to protect our coastline and our maritime boundary of Alaska, which is so important to all of us. Over half of the fishery resources in the United States are in the north Pacific, and the Admiral has had a commitment and a dedication to protect those resources.

When our Nation needed Admiral Loy's expertise to secure our transportation systems after September 11, he answered the call to service and assumed a newly-created post of Deputy Undersecretary of Transportation for Security. In 2003, he became the administrator of the Transportation Security Administration and assumed the critical task of securing every facet of our Nation's transportation system. Admiral Loy successfully led TSA through the transition into the Department of Homeland Security, and furthered his agency's dedication to security while improving public outreach and customer service.

I do believe that I know of no man more qualified to take over this position than Admiral Loy. He has completed enormous tasks as though they were small tasks, and I think the Committee would

agree, the Admiral's experience and dedication will serve him well as the second in command at the Department of Homeland Security. I know of no greater honor than to ask the Committee to move very quickly on this nomination.

Thank you very much.

Chairman COLLINS. Thank you very much, Senator Stevens. Senator Inouye.

Senator INOUYE. Madam Chairman, I thank you very much. I wish to ask for your permission to have my statement made part of the record.

Chairman COLLINS. Without objection.

TESTIMONY OF SENATOR DANIEL K. INOUYE,[1] A U.S. SENATOR FROM THE STATE OF HAWAII

Senator INOUYE. As my distinguished friend from Alaska indicated, he has the longest coastline. The State of Hawaii is surrounded by water. We have all the services on our islands, but the most favorite service is the Coast Guard. It saves more lives. We are surrounded by fishermen all the time, men who go out and surf, and without the Coast Guard we would have crise every day. Thanks to them, our families are happy, people are happy.

Admiral Loy has had a long and distinguished tenure with the Coast Guard. He has been commandant for 4 years. He has led the Coast Guard through one of the most significant periods of transformation in the history of that service. He has improved the readiness of the operation. He is preparing for the future. For many, many years they could not maintain their recruitment level. He has exceeded that. He has exceeded in retention, and he has ensured the personnel were properly supported by the finest equipment possible. He has had the training and the background and experience that we sorely need in this new position.

So I am most pleased and proud to join Senator Stevens in commending Admiral Loy to you.

Senator STEVENS. Could I just add something, Madam Chairman?

Chairman COLLINS. Senator Stevens.

Senator STEVENS. In my State, the Coast Guard operates helicopters that fly over barren seas and barren areas that are one-fifth the size of the United States. His people deliver babies, they pick up stranded people from ice floes, they patrol to see that the foreign fleets do not come into our shores, and they are really great neighbors. I think the fact that we have this nomination before us today demonstrates the wisdom of the battle that you and I fought that you were speaking of when I came in the room. But now, by having Admiral Loy in the position he is going to assume, it shows to everyone that that commitment is a real commitment, to make sure the Coast Guard will survive and be really compatible with the whole concept of homeland security.

So I really welcome this nomination and the assurance it gives those of us who had some fear about putting the Coast Guard in this new Department. I hope you will move the nomination quickly. Thank you very much.

---

[1] The prepared statement of Senator Inouye appears in the Appendix on page 25

Chairman COLLINS. Thank you very much. I know that both Senators have other engagements and I am going to give you the opportunity to depart the Committee. But I want to thank you both for taking the time to be here and to endorse this nominee. Your endorsement means a great deal.

Senator INOUYE. Thank you very much, Madam Chairman.

Chairman COLLINS. I would now like to call on the other distinguished Senator from Hawaii, Senator Akaka, for his opening comments.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Madam Chairman.

Admiral Loy, you come before this Committee with high recommendations from two colleagues whose opinions I respect tremendously, my good friends Senators Stevens and Senator Inouye. I thank you for being here this afternoon, and I thank you for your visit with me earlier today.

Admiral Loy, as Administrator of the Transportation Security Administration and the former Commandant of the Coast Guard, you have served your country well. As was mentioned, you were in the Coast Guard some 40 years. You understand firsthand the unique challenges faced by the Department of Homeland Security, and the experience you have had in the Coast Guard certainly will make a huge difference in securing our country.

To be effective, policies within the Department must address the specific homeland security needs of each State and municipality. The State of Hawaii is over 2,500 miles from Los Angeles and is accessible only by plane or ship. It takes 5½ hours to fly from the mainland and 4½ days by sea. This distance makes mutual aid from mainland States or from other Pacific jurisdictions unfeasible. Hawaii is home to 53,600 military personnel and hosts about 160,000 tourists on any given day. I have joined with Senator Collins to ensure that first responder funding covers all who reside in a State including military and tourist populations. I look forward to working with you to ensure that this priority is addressed in first responder allocations.

As the head of TSA, you serve on the DHS human resource system design team which has forwarded its recommendation for a new personnel system to DHS Secretary Ridge and OPM Director James. I expect you to foster an environment of inclusion that brings together the different talents of Federal workers and the different cultures of agencies included in this new Department. Your experience tells me that you will.

As we protect America by reorganizing the Federal Government we cannot overlook the fundamental rights of Federal employees. Union representation, collective bargaining, and appeal rights whistleblower protections are all critical elements of a strong and stable workforce. The rights of Federal workers complement our ability to safeguard the country.

Our goal is to protect the Nation. The key to attaining this goal is skilled and highly motivated employees and capable leadership. If the imposition of a new personnel system results in a demoralized workforce and accelerated retirement by skilled workers,

then the question needs to be asked, is our Nation's security at risk?

There will soon be new personnel systems for the largest Federal agency, the Department of Defense, and the third largest, the Department of Homeland Security, which will bring massive changes to those personnel essential to our national security. Any changes have to be looked at more seriously, and I want your commitment to work with me to ensure that we protect the rights and benefits of our Federal workforce. Much of the debate has focused on union rights. I, for one, believe that a modern and agile workforce is not incompatible with collective bargaining.

Admiral Loy, you have an immense task before you. I commend you for accepting the responsibilities of this position, and I know you will continue to make significant contributions to protecting the people of our great country. I consider you as a tremendous plus for what we are doing to secure our country.

Thank you very much, Madam Chairman.

Chairman COLLINS. Thank you Senator. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you, Madam Chairman. Earlier, Admiral Loy, when Senator Stevens and Senator Inouye were jockeying, debating about who was going to go first and Senator Inouye mentioned that it was Senator Stevens' 80th birthday today, I thought the person at that table who really receives the best gift is you. To be introduced by either of them at a confirmation hearing is a great honor.

Admiral LOY. Indeed.

Senator CARPER. To be introduced by not one but by both of them is really quite extraordinary.

As an old Navy guy for 23 years active and reserve duty and someone who served for 10 years on the Coast Guard Subcommittee in the House of Representatives before I was elected governor, I just want to express my thanks to you for your service to our country, my great respect for the Coast Guard for the good they do in Delaware and the Delaware Bay, the Delaware River, and the Atlantic Ocean not far from where we live.

I am grateful for the work that you have done in leading TSA within this new Department over the last couple of years. And I appreciate the chance to have sat down with you and to have spoken earlier today about some issues and when we get into questions I hope to be able to revisit a couple of those. I will just mention them again.

One of those was the issue of the funding formula for first responders that Senator Collins and I have worked on. I would like to discuss that with you a bit more. Among the responsibilities that TSA has is not only aviation security and important transit security but also rail security and I would like to revisit that with you, if I might.

Finally, I would like to talk a bit more about the concerns that have been expressed to us by port workers. The Port of Wilmington—and I know you have heard these from workers in other ports—employs some people who have had problems with the law and have some criminal violations on their records. They have gone

straight. They have become law-abiding citizens and contributing members of our society, and a number of them have, I think, real concerns about their future as breadwinners for themselves and for their families. I would like to have a chance to delve into that with you as well. We will have a chance for that here shortly.

I want to thank you again for your service to our country and for your family to be willing to share you with the rest of us.

Admiral LOY. Thank you, sir.

Chairman COLLINS. Thank you very much, Senator. Senator Lautenberg.

OPENING STATEMENT OF SENATOR LAUTENBERG

Senator LAUTENBERG. Thank you, Madam Chairman. My respect for holding this hearing and dealing with this complicated problem of having a nominee about whom there is virtually no controversy. It is not usual that we do these things.

But also, I always think about New Jersey and its relatively enormous coastline for the landmass that we have. Then we get Hawaii and Alaska. Ain't nothing there but water. But the fact that you have enjoyed the universal respect, and I might even say, Admiral James Loy, the affection of people you work with, because it is not just a pleasing personality. You have taken to your tasks very well.

Few have had the rich experience that Admiral Loy has had. To come to this fairly complicated job, having been with the Coast Guard, and commandant, I think it equips you particularly well because for a relatively small agency they have more responsibilities, the Coast Guard. And it is constantly enlarging the responsibilities without commensurately enlarging the budget. The Coast Guard has, I think, performed miracles. When you think of all the duties they have, everything from ship manifests, to pollution control, to illegal refugee movements, the drug enforcement, to picking people off the high seas, and to contributing as well to being a good neighbor to make sure that things operate well.

We are very fortunate in the State of New Jersey to have the Coast Guard training base there. Admiral Loy and I had a fair amount of contact in his days as the Coast Guard commandant and it was always a pleasure to see him and to hear from others who served with and for him, the respect that he enjoyed.

Having said all those nice things now I want to get down to the nub of some things that we are going to have to be concerned about. One of them was mentioned by our friend from Delaware, and from Hawaii as well. I served as the commissioner of the Port Authority before I came to the U.S. Senate so I know quite a bit about how the port operates, its importance to our economy, its vulnerability to terrorism.

By the way I mentioned, Admiral Loy, yesterday we had a chance to chat, to see a couple of Coast Guardsmen out there post-September 11. The Hudson River compared to the Atlantic Ocean may not look like a place that you have got to worry about, but there is an awful lot of ship traffic, a lot of turbulence in that river because of the ship traffic. Out there in a rubber dinghy with a machine gun mounted, making sure that they did whatever they could to protect us and to protect the commerce that goes through the

harbor. The Coast Guard estimated that they needed $963 million this year and $4.4 billion over the next 10 years to make our ports safe. I hope that Admiral Loy, in his new post, can pry that money loose.

The question of first responder grants, for me a particular concern in the State of New Jersey was that our State and our neighboring State New York, suffered the most on September 11 directly. We are ranked near the bottom per capita when the money was doled out. Some of that stems from a faulty allocation formula embedded in the USA Patriot Act, but to his credit Secretary Ridge has acknowledged problems with the formula and we still need to fix that.

There is another element that concerns me and that is our color-coded threat system. It does not do much, and if we do not scrap it altogether, we need to revamp it considerably. Because to issue threats that have no support or no advice as to what you do, where do you go? I have had these silly calls. I think they are silly because I believe that we are doing largely what is necessary. But when a threat comes out and I get calls in our office, dare we go to New York City now; or dare we go here; or dare I take my kids on vacation, it is not the way to do things. It just alarms everybody without offering any solution.

Another problem that I am concerned about is with the air marshals. Now I am concerned that the principal security inspectors are allowing flight attendants to take home study courses as part of their security training, but more concerned about what is happening to our Federal air marshal program. It is up, is it down, with regard to budget cuts and so-called cross-training with Customs agents. I am not quite sure what the intentions are. At one point they said they would get rid of them. Then I saw they were bringing them back. I think we ought to firm up that program. It is a very important protection that we afford the flying public, and we want to make certain that that is manned to the proper degree.

Last, the new threats that seem to arise. Whenever you think you are working on the things that really count you find out that there is another leak in the dike, and this one is surface to air missiles. A year ago this month the world saw the SAM attack on the Israeli jet in Mombasa, Kenya. And more recently, a sting operation in the port of New Jersey, port of Newark, we revealed an attempted to smuggle SAMS into the port. They were almost boastful about how they got into it. The prosecution was there and it will be taken care of, but the fellow who they caught with this was determined to create a structure, an organization to bring these things in on a regular basis. How devastating. So these weapons may present the biggest terror threat to commercial airliners and I want to know what the administration is prepared to do to address it.

Madam Chairman, I will spare you the time and the Committee. Those are a few of my concerns, raising them, I want to suggest that we have to go further to make our country safer against the scourge of international terrorism. But I think Admiral Loy is equal to the task and I look forward to confirming him as I know others do as well. We wish him well in this very important task.

Admiral LOY. Thank you, sir.

Chairman COLLINS. Thank you, Senator.

Admiral Loy has filed responses to a biographical and financial questionnaire, answered prehearing questions submitted by the Committee, and had his financial statements reviewed by the Office of Government Ethics. Without objection, this information will be made part of the hearing record with the exception of the financial data which are on file and available for public inspection in the Committee's offices.

Admiral our Committee rules require that all witnesses at nomination hearings give their testimony under oath, so if you will please stand and raise your right hand.

[Witness sworn.]

Admiral Loy, do you have a prepared statement that you would like to give at this time?

Admiral LOY. I have a prepared written statement, ma'am. If I could submit it for the record, I would appreciate that, and just provide perhaps a couple moments of oral comments.

Chairman COLLINS. It will be included in full.

TESTIMONY OF ADMIRAL JAMES M. LOY,[1] TO BE DEPUTY SECRETARY OF HOMELAND SECURITY, DEPARTMENT OF HOMELAND SECURITY

Admiral LOY. Good afternoon, Senator Collins and Senator Akaka, and all Members of the Committee. Thank you for scheduling this hearing so quickly and giving me the opportunity to appear before you today. I also want to thank Senator Stevens and Senator Inouye for their kindness in sponsoring my nomination today. Both represent to me the epitome of public service and our work together for many years on Coast Guard issues really now represents a foundation of capability our Nation needs to secure our homeland.

I am honored that President Bush has nominated me to serve alongside my good friend and fellow Pennsylvanian, Secretary Tom Ridge, as the Deputy Secretary of Homeland Security, and if confirmed I will do my utmost to serve the President and the Secretary in protecting our homeland from acts of terrorism, as we also maintain our way of life and all the freedoms that we enjoy as Americans, and to preserve and expand our national economy all at the same time; a difficult set of challenges.

I have the singular experience of having led the two largest organizations that comprise the Department of Homeland Security, the Transportation Security Administration and U.S. Coast Guard. Together they include approximately 100,000 dedicated men and women, more than half the DHS workforce. This gives me a unique perspective, I believe, on the challenges we face in molding the Department into a fresh, cohesive agency. If you will, having looked from the bottom up, I will be able to bring those thoughts and lessons learned into the dialogue of the leadership of the Department. I hope that perspective will be valuable as we move forward together.

Madam Chairman, with your permission I would like to just mention four quick things that I think are important to the funda-

[1] The prepared statement of Admiral Loy appears in the Appendix on page 00.

mental success of this new Department, this new adventure called the Department of Homeland Security.

First, information sharing and analysis. If this Department is to succeed we must build the capability to collect, to share, to analyze and to distribute the intelligence and information sets necessary to secure the homeland. I think this will be very different from anything that we have ever been expected to do in the past. We must design, if you will, a common information picture such that all gathered information is available to analyze, that all analyzed information becomes actionable products, and that all those products gain distribution to those who can best put them to use to secure America.

Second, the notion of critical infrastructure must become the product of criticality assessment on one hand, vulnerability assessment on the second, threat assessment on the third, and then very real, methodical risk management as a fourth dimension of how to grapple with this challenge of identifying and securing the critical infrastructure of our homeland.

Third, this Department must become the model Cabinet-level agency for the 21st Century. We have every opportunity to do that. Organizational excellence must become the norm across the board in all our operating agencies as well as in our support structure. We must demonstrate with solid metrics that we are doing our work efficiently, effectively, and with an eye to the good stewardship of the taxpayer's dollar.

Fourth, we must accept the challenge offered by the national homeland security strategy and interpreted boldly and widely for the American public, and especially for our workforce at DHS. That means each of us entrusted with positions of leadership must be bold and directive and methodical as we set goals, as we optimize objectives and design systems to accomplish the departmental mission. And second but simultaneously, to build the cultural norms expected in a high-performing organization.

I spent all my professional life in one such organization where the core values of honor and respect and devotion to their duty meant something visceral and real to every sailor in that organization. We are working hard now to build that same culture at the Transportation Security Administration, and it must also be done at DHS. I look forward to taking on that challenge with Secretary Ridge.

Last, I offer the simple notion that we are all in this together. Our strategies and plans must be open to all of those with good ideas. Our reach must include State, tribal, and local and private sector players. Securing the homeland is an obligation now for every citizen of this great Nation. The events of September 11 show that terrorists draw no distinctions between military targets and civilian office buildings. This is a gravely different security environment that we are living in post-September 11. It calls for creative thinking, diligent research, and a collective commitment to hold the edge and to keep complacency at bay, because indeed I believe to some degree it was complacency that got us into trouble over the decade post-1989 after the fall of the wall and after the dissolution of the Soviet empire took away that single superpower that we were vying with.

I am very aware of the seriousness and the importance of the challenge and opportunity that President Bush and Secretary Ridge have entrusted to me, and if confirmed I pledge to bring tirelessly whatever I have learned to the task.

Thank you again for your sensitivity to the scheduling of this hearing and I look forward to your questions.

Chairman COLLINS. Thank you, Admiral Loy. I am going to start my questions with three standard questions that are posed of all nominees. First, is there anything you are aware of in your background which might present a conflict of interest with the duties of the office to which you have been nominated?

Admiral LOY. No, ma'am.

Chairman COLLINS. Second, do you know of anything personal or otherwise that would in any way prevent you from fully and honorably discharging the responsibilities of the office to which you have been nominated?

Admiral LOY. No, ma'am.

Chairman COLLINS. Finally, do you agree without reservation to respond to any reasonable summons to appear and testify before any duly constituted committee of Congress if you are confirmed?

Admiral LOY. I do so pledge.

Chairman COLLINS. Thank you. We will now start with the first round of questions limited to 7 minutes each. I would ask my colleagues to help me with the time limit and we will do a second round if needed.

Admiral Loy, in my opening statement I raised the issue of border security, which is one of the greatest challenges facing DHS. Each year the United States legally admits millions of non-citizens through our borders. In Maine, some 4.6 million cars and trucks cross over the border from Canada each year. That is a lot of traffic and obviously the Department is very concerned about opportunities for terrorists to exploit weaknesses in border security.

But there was a flip side to the coin. For many Maine residents who live less than an hour's drive from the Canadian border, traveling back and forth between Maine and Canada is a way of life. Family members live across the border from one another, businesses in one country depend upon suppliers and customers from the other in order to survive. Sometimes the border in Maine literally runs through a neighborhood, or on one side of the street it is Canada, on the other side it is the United States.

Last year, to try to tighten border security, the Department eliminated the Form 1 and the port pass programs which allowed American residents to use unmanned border crossings 24 hours a day. This was very important to a lot of the residents living in remote areas of my State who depended upon those two programs for access to medical and religious services, family events, social activities, the grocery store, the hospital which are on the other side of the border. I would like to give you an example to illustrate the problems that the elimination of those programs have caused in my State.

There is a small border community in Quebec called St. Pamphile. On the U.S. side of the border there is no development, only miles and miles of woods that produce timber for processing at the mills in Quebec. But there are some Maine families who live

on the U.S. side of the border and they depend upon services in Canada. Everything they need from the grocery store to the hospital to the church is on the Canadian side, including emergency services. The problem is that once that program was eliminated and the gates were locked, the residents on the Maine side of the border are essentially prohibited from crossing the border after 5 o'clock. They cannot go at all on Sunday because the gates are locked.

This is a real problem. The residents are very frustrated by this. They are obviously law-abiding American citizens. They would be the first to point out any suspicious character in their midst. This has changed their entire way of life.

I think ultimately technology is going to be the answer to this problem where we can have some sort of biometric passcard and perhaps remote cameras to check out who is crossing. But in the meantime this is creating tremendous hardship in this one community for the 50 or so residents who live on the American side. But it is a problem for other remote border communities in Maine too.

I would ask that you make a commitment to work with me to try to come up with a solution that meets the need for tighter border security while at the same time acknowledging the fact that these individuals who are law abiding, who have lived here their entire lives in some cases, now find that their movements are greatly restricted. They would have to drive an extraordinarily long distance to get to the next manned border crossing. We have been working with the Department on this but we have yet to be able to come up with a solution.

Admiral LOY. Madam Chairman, I am happy to pledge to work with you in trying to find a better solution to the circumstances you describe. I think this dual goal set that you just described so well of security on one hand but holding onto that way of life that has become so critical to people just a couple hundred yards or just a mile or so away are legitimate challenges that we have to find better ways to deal with.

I think the smart border accord that has been a very fundamental exchange between Canada and the United States at the diplomatic level, and Secretary Ridge and Minister Manley have literally, each month since about 18 months ago, looked carefully at a list of about 30 objectives that they have to make such things happen better between the two countries. I even think that further down the road there is a likelihood of a notion referred to as a North American initiative where the real borders we are concerned about are the borders that circumvent the entire continent, let alone those that are binational in nature between Canada and the United States, and between Mexico and the United States on the southwest border as well.

I do believe that there are technological possibilities that can help us with this on the other end of the timeframe, and at the same time reinforce the legitimate concerns that we do have for our own borders. Whether there are hours that we can play with here in terms of the openness of those border crossings, I will be happy to take back to the Department and review there the concerns that you have expressed to me and work with you to see if we can find a better answer.

Chairman COLLINS. Thank you. I appreciate that commitment.

Earlier this year, the Committee held a hearing that focused on the threat to our Nation's ports which I view as one of our greatest vulnerabilities. I have a series of questions I want to ask you about that but in the interest of time let me cite one particular concern. In June, I wrote to Secretary Ridge to express my concern about the Department's proposal to allocate some of the money that had been designated for port security by Congress for other purposes. I was pleased in response to the concerns that many of us raised that that decision was reversed.

As we anticipate a third round of port security grant announcements I am pleased to hear that the TSA is poised to distribute $105 million that is still left over. But once again there are these rumors that the Department only plans to release a portion of the 2004 funding in this round. I would like you to address that. I think it is imperative that we make a real effort to upgrade security at our ports.

Admiral LOY. I could not agree with you more, ma'am, as my immediate last 8 months in uniform were all about maritime security design efforts in the wake of September 11. Port security has been something that is of great personal interest to me as well. You are referring, of course, last year to enormous and very consequential budget challenges that we had to fight our way through at the Transportation Security Administration and to whom those dollars for port security grants had been appropriated for distribution. In the spend plans over the course of that year where literally at the 364th day of that fiscal year I as the administrator for TSA, was still looking for an approved spend plan for that fiscal year. That was the nature of the challenges that we had to actually, potentially reprogram funds from purpose A to purpose B just to get through the fiscal year.

I think it was all about what has classically been the case historically in our country, in the wake of a tragedy when the Congress passes a piece of legislation and the administration tries to figure out how to execute that piece of legislation, and sticker shock sinks in, and then we literally work a couple budget cycles to find out the true job description and the resource base necessary to do that work. We are still grappling with that at TSA as this year plays out as well.

But with respect directly to the port security grants, as you know, all of them were in fact reissued for fiscal year 2003. The $105 million you speak of is actually the monies that were in the supplemental from the previous year that really were round two but are becoming round three. This distinction that you are making between $75 million and all of the $125 million set aside in fiscal 2004, this is the reasoning behind why we are edging it at $75 million at the moment.

The application process for the third round of grants was to the point where we had about $1 billion worth of requests coming in. I am very proud of the process that we have designed. There was local review with the harbor safety committees involved in how to make sure that the applications going forward were rated in such a fashion that all of the players in that locale would see the value of that application. Then there was a regional review and finally

a leadership review at the top between MARAD, the Coast Guard and TSA.

When we categorized them, they fell into logical categories of one, two, and three, and this $75 million worth of the 2004 appropriation will simply enable us to fund all those who we rated in category one. Then the balance of the $50 million will become available to another round of port security grants on into the fiscal year. That is the intention at the moment and no mischief afoot here as it relates to potentially trying to reprogram these dollars.

Chairman COLLINS. Thank you. Senator Akaka.

Senator AKAKA. Thank you very much, Madam Chairman.

Let me begin my round of questioning by affirming that collective bargaining rights are compatible with national security. Providing Federal employees with a meaningful voice in the workplace is a smart business practice that will enable any agency the ability to attract and retain a motivated workforce. The Homeland Security Act requires that the Department must, "ensure that employees may organize, bargain collectively, and participate through labor organizations of their own choosing in decisions which affect them, subject to any exclusion from coverage or limitation on negotiability established by law."

Admiral Loy, how will you determine whether DHS employees may bargain collectively?

Admiral LOY. Senator, the plan for which this new HR system will be designed has gotten to a point where it is just about to be offered to the Secretary for his decisions. We have been, I believe, extraordinarily inclusive in the process to date in terms of making certain that voices were heard from the workforce through focus groups, town hall meetings that were held around the country, and where in the holding of those meetings it was not a management representative that went out and held a meeting and then brought whatever information back. But rather it was teams composed of those members of the design team that had been assigned, including their union representation from the three unions that represent Federal workers in the Department of Homeland Security.

I was asked to be a member of the senior review committee by Secretary Ridge in my position as the TSA administrator, as were a number of other senior players in the Department: The director of the Secret Service and the Commissioner of BCP. All of us met for several days, listening carefully to the work that the design team had put together, and our colleagues at that table included the presidents of the three respective unions as well. So the voices have been heard very inclusively to this particular point in time. Just 2 weeks ago an opportunity was provided again to the three union presidents to meet personally with Director James at OPM and Secretary Ridge at DHS to have those two people hear what the concerns may be of the respective union representatives having been a part of this process all the way from the beginning.

As you know, the legislation restricts us to actually grapple with about four or five key elements of any HR system, those being pay and compensation, performance management, adverse actions and appeals, and labor relations. Those are the areas that the new design effort will be allowed to grapple with, leaving in place all those enormously important things that have become part and parcel of

American labor relations over the years, including whistleblower protections and merit foundations, respecting inclusiveness, all those things that we want very much to be part of the system.

The next challenge, sir, is to have the Secretary hear out his design team with those areas in mind. We want that to be an inclusive process as well so that workers as well as their representatives from the three unions are part of the team that continues to do the design work once the Secretary has made his judgments about the new system. So I am very pleased with where we are so far, sir, and commit to you and to the Committee that we will meet the specs that have been outlined for us in the law.

Senator AKAKA. Thank you. I also have a question regarding the DHS Bureau of Immigration and Customs Enforcement known as BICE. In response to questions my staff raised with the director of operations at BICE last summer, I understood that BICE planned to conduct a review of its June 9 reorganization and would brief Congress after 90 days. To date we have not received this briefing. Do you know the status of the review?

Admiral LOY. Senator Akaka, as I sit here I do not know the status of the review but I will be happy to take that back as a question from the dais and find out where that review is at the moment and get information back to you quickly.

Senator AKAKA. Thank you. During testimony before this Committee a couple of months ago, the Office of Domestic Preparedness Director stressed that communities should improve their States' homeland security by working together to combine resources across State lines. However, unlike all States but Alaska, external assistance from the U.S. mainland is not immediately available to Hawaii. As deputy secretary how would you ensure that any regional approach fully addresses Hawaii's homeland security?

Admiral LOY. I think we have to understand, Senator Akaka, what is our fundamental goal. Our fundamental goal is to make certain that the people of all 50 States are cared for properly with respect to the design work associated with our homeland security goals. Any kind of regional notion that makes very good sense, for example, in the region of Pennsylvania, New York, and New Jersey where they all come together, there are regional issues there that can be very well served by mutual effort between and among those States.

The notion of regionalization, however, must never fail to include the State of Hawaii simply because geographically it is not attached to what would logically be a region. It may be a region of its own. To that end, sir, we will absolutely commit to ensuring that Hawaii as a State and the people of Hawaii are dealt with in the very same supportive fashion, whatever the Federal programs might be, that would get to other States in a regional sense.

Senator AKAKA. Thank you. My time has expired, Madam Chairman.

Chairman COLLINS. Thank you, Senator. Senator Carper.

Senator CARPER. Thank you, Madam Chairman.

Admiral, I telegraphed earlier the three issues I wanted to explore with you. Before I do that let me just ask on a more personal note to talk about values, the values on which your leadership is founded. You mentioned a couple of those in the course of your ear-

lier remarks—honor, respect, and so forth. When I was privileged to be governor for my State we tried to build an administration based on four or five core values: Figure out the right thing to do; do it. Just be committed to excellence in all things. Golden rule, treat other people the way we want to be treated. Never give up. I believe when things go well to give the credit to other people. When things go badly, accept the blame. I always seek to surround myself with people smarter than me.

Admiral LOY. Which is easy for me, sir.

Senator CARPER. When I was in the National Governors Association—I have actually mentioned this to at least Senator Collins before. The National Governors Association, when you are elected as a new governor you got assigned a mentor, somebody who is already a governor, and usually within the same party. I was assigned Tom Ridge. I had been elected in 1992 Governor of Delaware and in 1994 he was elected Governor of Pennsylvania. He and I were friends and had been friends since our days in the House of Representatives in 1982. But as his mentor I sought to instill in him the kinds of values that I just alluded to earlier. One of those was to always surround himself with people smarter than him. I guess I would just ask at the start, would you characterize yourself as smarter?

Admiral LOY. Than Governor Ridge? I would not go there in a heartbeat, sir, but I thank you for the opportunity. [Laughter.]

Senator CARPER. Talk to us about your core values.

Admiral LOY. Yes, sir. All of those that you mentioned are, I think, enormously important. I believe that there must become an ethos in an organization that allows individual accomplishment to feed the well-being of the organization and, therefore, the accomplishment of its mission.

I was privileged to be the chief of the personnel shop in the Coast Guard back in the early 1990's and one of the things we initiated was a leadership development program that I believe is now second to none anywhere in the Federal Government. It is housed at the Coast Guard Academy where it recognizes the contribution of not only the senior leaders in terms of officers but breeds in the cadet corps, the future leaders of that organization, the great strengths of the chief petty officers and the young petty officers that make a difference in the bowels of any organization; those kids on the hangar deck, those kids that are taking that 47-footer out in that terrible storm to pull off that rescue.

I believe there are fundamentals to all of us, whether that is a Western ethic or whether it is one fundamentally just based on those things that, in my case, I was so fortunate to be brought up to value by my parents, and by scoutmasters and people who cared for my well-being as a young person and did whatever was necessary to make sure I did not fail to learn those lessons.

This is not something that is rhetoric for me. This is something that I believe in very deeply and try hard to instill, just in a couple phrases, what might be of value to the rest of the organization. At TSA our values are not honor, respect, and devotion to duty, which are the values of the Coast Guard. And you may know what they may be for the Navy, or you know what they may be for the Marine Corps.

But at TSA I felt it was incredibly important for us to have integrity, innovation and teamwork as our values because what we were doing for the Nation became an opportunity to breathe life into those words so every screener at every airport, every supervisor looking out for the well-being of those screeners took seriously the ethic associated with a couple of simple words that could become so meaningful if allowed to be broadcast widely to the organization at large. I look forward to an opportunity to find that cultural foundation in DHS and broadcast it widely.

Senator CARPER. I think you are going to have that opportunity. Let us talk about rail security for a bit, if we could. We are mindful every time we go through an airport or ride on an airplane of the work that TSA has done under your leadership with respect to making air travel safer. We are aware at the Port of Wilmington, and other ports, of the work that has been done to make our ports and the shipping of goods in and out of those ports less hazardous. I understand that the Department of Homeland Security is working on, I think it is called the national transportation security plan. I think it is going to be released sometime maybe the middle of next year. Any idea how this plan will address freight rail as well as passenger rail security?

Admiral LOY. Yes, sir. We are working hard at TSA to build a national transportation system security plan, recognizing that it is a puzzle piece that has to first and foremost fit into the larger puzzle that the Secretary is responsible for in the other 12 economic sectors and four asset categories that are outlined in the national homeland security strategy. So as that big puzzle goes together I am obligated as the TSA administrator to make certain that the transportation piece fits well there, because there are intersector challenges.

I have been to, I do not know how many tabletop exercises over the last 2 years where the focus may be on a chemical plant security scenario, or a nuclear scenario, or a scenario even dealing with something like banking, or food and agriculture kinds of challenges. What is invariably the case is that the transportation sector gets involved in that tabletop exercise because whatever might be accomplished to either respond to or restore the well-being of the Nation in that process requires transportation in order to get that done. So there is an intersector kind of connectivity there that the Secretary has to be aware of as he composes that bigger puzzle.

My piece, however it is shaped to fit into the Secretary's bigger puzzle, is also a complex one made up of aviation, maritime, rail, highway, transit systems, pipelines, those elements of the transportation sector that have to also fit together. There are intermodal challenges there. That container that comes from sea and gets on a train and eventually on a truck to go to Iowa City has to be recognized as an intermodal challenge with respect to the security of whatever is in that container.

So the national transportation system security plan will be the opportunity to talk about standard-setting, vulnerability assessments, mitigation strategies, and compliance means by which we can comfortably fit the transportation puzzle together such that it fits well into Secretary Ridge's greater challenge.

As to rail, sir, it is not a matter of waiting for the next 6 months or whatever. We have been doing a lot of very good and worthwhile outreach to the rail industry already. There have been critical asset inventories taken of rail infrastructure across the country. Amtrak, and the American Association of Railroads, and the Federal Rail Administration, and DOT and TSA have worked together on those projects. Amtrak and class one rails, the bigger rail services, have developed an information sharing center, ISAC, Information Sharing and Analysis Center that affords a chance to send information to them for distribution to the industry, and gather information from the industry through the ISAC back into the TSA so we can share it with the intelligence and information aggregation process that I think is so critical to what we are doing in this new Department.

So whether it is the notion of learning from the rail industry that it is not about prevention exclusively, but it is perhaps also about restoration. I took a train ride to Wilmington from Washington.

Senator CARPER. Great ride, is it not?

Admiral LOY. Yes, sir, it is. But I was given the chance to sit up there in the front cab with this wonderful, crotchety old guy who had been driving that route for years, and he helped me understand that it was not necessarily about prevention in the rail business. Yes, prevention at the terminals and those things are needed. But he asked me things like, Admiral, have you seen a police officer? Have you seen a fence? Have you seen a camera? Have you seen any of those kinds of things along this—he was talking about 50 miles out of Washington, but referring to thousands of miles of rail line across the country, railbed across the country. He made it clear to me that restoration is the fundamental reality in the rail business that is different than other elements of the transportation sector. So it literally reshaped my thinking in putting a strategic plan together for the transportation sector.

So we have done some very good things. AAR, American Association of Railroads, is a marvelously impacting trade association for that industry and have been terrific in coming to the plate and helping us figure those things out.

Senator CARPER. Good. My time has expired. If I could just add a closing statement, Madam Chairman.

Chairman COLLINS. Certainly.

Senator CARPER. Just keep in mind, Admiral, as you and your team work on this transportation system security plan, keep in mind that more people take the train today between Washington and New York than will fly on all the airlines combined, that during the course of this day hundreds of thousands of people will be in those tunnels underneath some of the waterways that we were talking about earlier going in and out of New York, and that at any one time during the day there are more people in those tunnels than in, I think, seven 747 aircraft.

Senator Collins and I have worked trying to come up with a funding formula for first responder legislation. I will not get into that any more. We have discussed that and we welcome your input. Last, just keep in mind, please, going forward the people who work in our ports, and sometimes in hard labor positions, a lot of physical labor positions, people who have made mistakes in their past,

who have a criminal record, who have gone on and made something out of their lives. So make sure that as we attempt to provide for better security at our ports and introducing this identification card program that we do not needlessly put at risk their livelihood and their ability to make a way for themselves and their families.

Admiral LOY. Absolutely, sir.

Senator CARPER. Thank you. Thank you, Madam Chairman.

Chairman COLLINS. Thank you. Admiral, another challenge facing the Department is striking the right balance between privacy concerns and security. Recently, the Department's chief privacy officer began an investigation of the role, if any, the TSA personnel may have played in assisting an Army contractor, Torch Concepts, in obtaining personal data from passenger records on over one million customers of Jet Blue Airways. I am sure you are familiar with that case.

Admiral LOY. Yes, ma'am.

Chairman COLLINS. First, do you know yet whether any TSA personnel were involved in encouraging Jet Blue to provide this private data on its customers to the DOD for the research project or to the contractor?

Admiral LOY. Madam Chairman, my understanding is that if there was TSA involvement, it was the bringing of the two together, not with respect to what might actually occur once they got together. But it was almost an invitation kind of thing, and an association kind of thing where Jet Blue and the contractor were introduced, if you will, to each other by TSA but without any value judgments on the part of the TSA personnel.

We are looking at that very carefully and I would probably be remiss in trying to speculate what might end up at the other end of the investigation that is underway, but the important thing here to me is to have it become that lesson that reinforces, as Jet Blue found out in this instance, that having violated their own privacy gameplan and rules and regulations that they had in place in the company, they got burned at the other of the day. And properly so, I might add.

At the other end of our day at the Federal level, for example, in our Computer Assisted Passenger Pre-screening System, CAPPS–II, the privacy implications of that system must be inviolate at the other end of the day with respect to our concerns for probably six or seven areas that are properly challenging us to make sure we got it right before there is any switch turned on, so to speak, with this new system. This new system is going to be probably one of the most important projects we finish and put on the line for our country with respect to the security of the aviation system.

Having said that, we should never turn that switch on until those privacy concerns about effectiveness, about redress opportunities, about appeal rights, about mission creep, about all those issues that are enormously important to the privacy community are properly dealt with. The Congress has made that quite clear. In our appropriation bill this year there are eight areas that we are obliged to work with GAO on and return by February 15 in order to continue the testing of the system that will prove its effectiveness after February 15. We are on track to do that and I hold that as one of our most important chores.

Chairman COLLINS. I appreciate that update and your assurance that before the CAPPS–II system goes into effect that there will be a lot of thought given to the appropriate safeguards that need to be included. I think it is also important that those safeguards be in effect during the testing of the system because it is going to be difficult to test the system without access to the same kind of real world passenger data, that got Jet Blue in trouble. I would also ask you to keep that in mind as you proceed.

Admiral LOY. Yes, ma'am. It is not only the domestic side of the house, but there are very real issues associated with international PNR data, passenger name record data that are challenges to us at the moment that we have to get through before we can make the system viable.

Chairman COLLINS. I would like to turn just quickly to an issue that both Senator Stevens and I raised, and that is the role of the Coast Guard. As you know, Senator Stevens and I worked hard to get language in the authorization for the Department of Homeland Security to ensure that the traditional mission of the Coast Guard would not be jeopardized as it took on new and expanded responsibilities for homeland security. Just last month Maine suffered the loss of four more fishermen at sea who were on the Candy B II. That has been a real tragedy for our State and the Coast Guard's search and rescue mission. The search and recovery mission in some cases is just so critical to my State.

Could you give us an update of your assessment on how well the Coast Guard is doing in this new post-September 11 environment, whether it does have sufficient resources to take on these new responsibilities without compromising its vital traditional missions?

Admiral LOY. As you might imagine, I am very personally invested in what I know to be perhaps the greatest attribute that organization brings to our country, and that is the flexibility to go from almost crisis to crisis on any given day, but to go from where the Nation needs it best on day two to where the Nation needs it best on day three.

For example, on September 10, 2001 we were spending in the Coast Guard somewhere around 3 or 4 percent of our appropriated capability operationally on what I would call classic homeland security activity. Two days later we were spending about 53 percent of our appropriated capability on what became the crisis of the moment for our Nation. I think that is the good news and the bad news.

The good news is that it is yet again a demonstration of the flexibility of that organization to go where the Nation needs it. The challenge is how quickly can you return to whatever you perceive normalcy to be the day before the tragedy. I think with this particular tragedy, that old normalcy we will never see again. So our challenge is to provide the resources necessary to this service to find that new normalcy where heightened address of homeland security realities are there as well as the continued service in fisheries and counternarcotics and all the other missions that are operationally dependent—or the Coast Guard is the provider of those services for our country.

One of the most important projects in that regard is the Integrated Deepwater System project which offers the modernization of

that service's offshore capability. That modernization will provide the Coast Guard the wherewithal to do better search and rescue, to do better national defense, to do better homeland security, to do better fisheries, to do better everything that it does in that environment 50 miles or more offshore, and be interconnected with the coastal realities that are so much a part of our homeland security missions today.

I spoke with Admiral Collins just last week for the first formal time in getting ready—that rookie that took over after I left my job. He is doing a marvelous job with the organization and has been in fact supported by the Congress very well, I believe, in the last two budget cycles to provide him the tools to do this new homeland security job while he continues to provide those services that America has come to count on the Coast Guard to provide.

Chairman COLLINS. Before I yield to my colleague I just want to indicate to you that Senator Lieberman and I recently wrote to the OMB Director suggesting that the deep water project be accelerated and funded over 10 years rather than 20 years. It actually saves money in the long term and you get the capability. But I will not put you on the spot by asking you whether you would support that change.

Senator AKAKA. But you could, Senator. [Laughter.]

Thank you very much, Madam Chairman. I would like to ask about FEMA. The Department of Homeland Security now includes FEMA, which among its many responsibilities administers natural disaster mitigation grants. This multitasking has raised concerns that FEMA's emphasis on terrorism may result in a lower priority for natural disaster mitigation.

My question is, will you work to ensure that natural disaster mitigation grants, which Hawaii and so many other States rely upon, are not shortchanged as the result of FEMA's move to the Department of Homeland Security?

Admiral LOY. Indeed, I will, sir. One of the chores the Secretary had asked of me about 6 or 7 months ago was to take on the responsibility to design the new national response plan and the national incident management system for our country. It is an all-hazards plan. So the notion of whether it is a tsunami on its way to, God forbid, some island in Hawaii, or fires in the west of our country, or hurricanes as they go by, those natural disasters of the past are every bit spoken for in the design work of this new national response plan and national incident management system.

Furthermore, I think we are enormously proud of what FEMA has been able to do in just this past year in the new Department in responding to the fires in California, as well as the hurricanes that have gone by.

In California, I know that Mike Brown was out there personally day in and day out, and within 24 hours of the State being recognized for relief was actually writing checks to California State individuals for the challenges that they had undertaken through the course of the fires. So I feel very good about demonstrated behavior already and the planned inclusion of all hazards, including those that you described, sir, is very much a part of the Secretary's intention.

Senator AKAKA. The General Accounting Office added the consolidation of the Department of Homeland Security to its high risk list this year, partially as a result of the existing management challenges of entities included in the Department. At the same time, the Department is subject to the President's management agenda which includes competitive sourcing as one of its five components.

My question is, given the challenges of consolidation do you believe that contracting out goals are appropriate for the Department? If so, why?

Admiral LOY. I certainly believe that the notion that there are skills and competencies that have been honed to a higher level in the private sector compared to the Federal sector is a legitimate thing for us to address and sort our way through. On those occasions where the American public can be served better by outsourced functionality we should be about the business of doing that. That is, as you say, sir, very much a part of the President's management agenda which has four or five other aspects to it which we are equally zealous about taking on.

So the idea of making certain as we contemplate where some function is accomplished for the American public and being very methodical about the checks necessary to make those decisions methodically as well is part and parcel of the review process that gets us the answers to those on a one-at-a-time basis. It is not a blanket that is going to be strewn across the whole array of functions of the Federal Government. But where those things can be done better, I believe we serve the American public better by outsourcing them appropriately.

Senator AKAKA. I want to thank you very much for your responses, and I feel that we are so fortunate to have you in this position. You know that the government is setting new milestones and seeking flexibilities in governance in light of challenges that we never faced before. So it is going to be tough going and as far as I am concerned you are the man for it.

Admiral LOY. Thank you, sir.

Senator AKAKA. Thank you very much, Madam Chairman.

Chairman COLLINS. Thank, you, Senator.

Admiral I am just going to ask you one more question and then submit some additional questions on port security and other issues for the record. My final question for you has to do with the allocation of homeland security grant funds to first responders and to States and communities.

As I mentioned, this Committee has unanimously reported legislation that would make changes in the funding formula, but we would continue to provide a stream of money to each and every State because every State has homeland security concerns and vulnerabilities. I feel strongly we need to bring every State up to a minimum level before we could ever discontinue that funding stream. I often remind people that when you think of the State of Maine you think what a safe State it is, but in fact two of the hijackers on September 11 started in Portland, Maine. We are a State with an extensive coastline. We are a border State. That is why it is important that we provide some funding to every State and then look at specific threats, not just allocate on the basis of

population which may not have a correlation to the vulnerabilities and threats.

Do you agree with that general approach? I am not asking you to endorse specific funding levels or percentages, but that each State should receive a certain amount of funding?

Admiral LOY. Indeed I do. I think so, for the moment at least, until we can be much more sophisticated in how we would develop an algorithm that would take into account each and every State's requirements. When I got into this TSA position someone told me that when you have been to one airport, you have been to one airport. So the notion that the 450 airports that I would have to grapple with, each of them has a unique set of challenges. I believe our 50 States are like that in a way. When you have been to one State, you have been to one State.

The point there is that I do believe until we can reach a more sophisticated algorithm that would take that into consideration our default position for the moment must be a threshold level of funding for all States. Then it is an already sophisticated notion as to how you then distribute the rest. In my opening comments I tried to articulate criticality assessments, vulnerability assessments, and then this challenge of truly understanding what is being threatened, by whom and how, and what is the risk management that you are going to use to deal with that.

With respect to the balance of the distribution, I believe it should probably be around population density in some fashion because that represents a targeting value to the bad guys. We know that is the case. But I also believe that the inventory of critical infrastructure, however that is deemed in that State, should be part and parcel of the thinking in that algorithm. Then just what do we know from the intelligence going by that suggests that critical infrastructure, that population density is on the bad guys' targeting list for this year's grants as they go by. So criticality, vulnerability, the real sense of the threat, and then the judgment about how to manage the risk associated with that package, that becomes the means by which we distribute the balance of the funds.

I think in there somewhere is both support for your notion at the moment and a challenge to us to think our way through a better algorithm, if it is out there, for the distribution in the future.

Chairman COLLINS. I want to thank you for your testimony today, and I want to join Senator Akaka and my colleagues in thanking you for your willingness to serve in this extraordinarily vital post. You are taking on a huge responsibility and we are very grateful that you are willing to step forward. With your background not only in the Coast Guard but as head of TSA, I really cannot think of a better candidate for this position, so we very much appreciate your willingness to serve.

It is my hope that the Committee will be able to act expeditiously on your nomination and that we can have the full Senate move to confirm you before we adjourn for the year, which I hope will be sooner rather that later.

Without objection, the hearing will be kept open until 10 a.m. tomorrow morning for the submission of any additional written questions or statements for the record. This hearing is now adjourned.

[Whereupon at 4 p.m., the Committee was adjourned.]

APPENDIX

PREPARED OPENING STATEMENT OF SENATOR DURBIN

Madam Chairman, I am pleased that the Committee is considering the nomination of James M. Loy to be the Deputy Secretary of the Department of Homeland Security.

Admiral Loy has devoted his entire career—spanning nearly four decades—in service to our country. I commend his willingness to accept yet another challenge.

James Loy brings a refreshing sense of enthusiasm to the task ahead, along with expertise as a tested manager. The breadth and depth of his working knowledge of Departmental programs, as well as the challenges it faces, will serve him well. The American public will be ably served with his leadership and vision at the helm, working side-by-side with Secretary Ridge.

I know from our conversation last week the tremendous respect that Admiral Loy has for the dedicated efforts of the 170,000 Homeland Security Department employees who vigilantly protect our citizens, gird our borders and domestic infrastructure, and thwart terrorism on American soil. I certainly share those sentiments, and trust that, in assuming this new post, he will routinely engage that workforce as an essential partner in accomplishing the Department's mission.

I enjoyed the opportunity to meet with Admiral Loy last week to discuss several issues facing Illinois communities relating to transportation security, specifically passenger screening delays facing the Central Illinois Regional Airport and Chicago Midway Airport. I appreciated his interest and his offer to respond to those concerns, and look forward to their prompt resolution.

I wish Admiral Loy fair winds and calm seas in this new assignment, and pledge my support for his expeditious confirmation.

Thank you, Madam Chairman.

OPENING PREPARED STATEMENT OF SENATOR INOUYE

I am pleased to be here today to introduce Admiral James Loy, who has been nominated to be Deputy Secretary of the Department of Homeland Security. His long career in public service has prepared him well for this new challenge.

Admiral Loy wore the uniform of our Nation for more than 40 years as a commissioned officer serving in the United States Coast Guard. Admiral Loy began his career at the U.S. Coast Guard Academy, where every cadet learns the creed, "Who lives here reveres honor, honors duty." Admiral Loy not only learned the creed, but has also lived by that creed throughout his career.

Admiral Loy's long and distinguished tenure with the Coast Guard culminated with four years of service as Commandant. He led the Coast Guard through one of the most significant periods of transformation in the history of that venerable service, improving its readiness for the operations of today, and preparing for those of the future. After years of less than optimal recruitment levels, he rebuilt the Coast Guard's workforce to authorized levels and improved retention. Then, to ensure that these personnel were properly supported with the finest equipment possible, he oversaw the initial phase of the Integrated Deepwater System acquisition project, a systematic modernization of U.S. Coast Guard ships, aircraft, and sensors. This reinvigorated Coast Guard stands ready to fulfill its mission of protecting our marine environment and those that operate within it.

Admiral Loy's administrative experience will serve our Nation well in the Department of Homeland Security. As Chief of Staff to the Coast Guard, Admiral Loy redesigned the headquarters management structure. He also worked to focus the Coast Guard's planning and budgeting process on performance and results. His administrative skills were put to good use when he took over at the newly created Transportation Security Administration (TSA). Under his leadership, the TSA met every major deadline required to increase the safety and security of the American public

traveling our Nation's airways. This expertise will be a valuable addition to the Department which has been working to integrate many different agencies to serve our homeland defense.

I am confident Admiral Loy will continue to serve our Nation in the same exemplary manner he always has. I support his nomination to be Deputy Undersecretary of the Department of Homeland Security fully and without reservation.

Written Testimony of ADM James M. Loy
Senate Committee on Governmental Affairs
"The nomination of James M. Loy to be Deputy Secretary for Homeland Security, Department of Homeland Security"
November 18, 2003

Good afternoon Madam Chairman Collins, Senator Lieberman, and all of the Members of the Committee, and thank you for scheduling this hearing so quickly and giving me the opportunity to appear before you today. I also want to thank Senator Stevens and Senator Inouye for their kindness in sponsoring my nomination before you today. With me today is my wife, Kay, who has supported me with tremendous understanding throughout my many assignments during my long career with the Coast Guard, and now with the Transportation Security Administration. Kay, my children Kelly and Michael, and my two grandchildren, are the bedrock that gives me the determination to continue to serve my country.

I am honored that President Bush has nominated me to serve alongside my good friend, and fellow Pennsylvanian, Secretary Tom Ridge, as the Deputy Secretary of Homeland Security. If confirmed, I will do my utmost to serve the President and the Secretary in protecting the homeland from acts of terrorism, as we also maintain our way of life and all of the freedoms that we enjoy, and preserve and expand our national economy.

I have the singular experience of having led the two largest organizations that comprise the Department of Homeland Security - the Transportation Security Administration (TSA) and the United States Coast Guard (USCG). Together they include approximately 100,000 dedicated men and women, more than half of the DHS workforce. This gives me a unique perspective on the challenges we face in molding the Department into a cohesive agency. It also shows the challenges that we face in creating a new culture within the agency. The USCG is one of the oldest agencies in the United States Government with a long and proud history of more than 213 years, while TSA is one of the newest, having been created by Congress just two short years ago following the terrorist attacks of 9/11. Only the Department itself, created barely one year ago, is younger.

I have previously testified before many of the Members of this Committee in either my current position as TSA Administrator or in my prior post as Commandant of the Coast Guard, and I have met many other Members of the Committee in personal meetings. I have made it a hallmark of my career in public service to be forthright and accessible to the Congress and, if confirmed, I pledge to continue to follow this path. I appreciate the tremendous support this Committee has given to the President's efforts to protect our homeland. This support has made Secretary Ridge's job easier. I cannot stress enough how critical it is to our success to have the support of the Congress.

In the short time since March 1, 2003 when the Department actually opened its doors for business, merging most of the 22 former agencies that now make up the Department, we have accomplished much. But creating a new agency from the legacy organizations, and

protecting the citizens of the United States from threats of terrorism at home, is not a short-term effort. We are here for the long haul. The Department is still developing many of its policies and programs, which will mature in the coming months and years. If confirmed, I expect to assist Secretary Ridge in developing these policies and programs.

I know that a concern that many Members of the Committee have is to ensure that the functions of the Department that many consider not directly related to homeland security will continue. If confirmed I will support Secretary Ridge to ensure that this critical work for the national well-being continues unabated. The USCG, for example, will continue its superb search and rescue and boating safety missions even as it provides key support to maritime and port security. The Federal Emergency Management Agency (FEMA) will continue to provide disaster relief to stricken areas of the United States. FEMA, together with the many federal agencies that support its disaster recovery efforts, has performed outstanding work in helping our citizens recovering from the disasters of Hurricane Isabel and the Southern California wildfires. Agents of the Bureau of Immigration and Customs Enforcement continue to protect young people from child pornographers, alien smugglers, human traffickers, and other predatory criminals through its extremely effective Operation Predator. The U.S. Secret Service will continue to protect the President, the Vice President, other government officials and foreign dignitaries from all threats, whether or not they are related to terrorism, while also protecting the integrity of our currency system.

Foremost of our missions, of course, is to protect the homeland. Our DHS team members are dispersed throughout the far-flung corners of the United States, quietly doing their jobs every day. Whether it is at a lonely border crossing in Minnesota, or a known route for illegal immigration in Arizona, a port in Alaska or Hawaii, an airport in Maine or any of the 50 states, or a research lab perfecting radiation, chemical, or biological detectors, DHS employees are helping to keep us secure. If confirmed, my job in Washington is to make it possible for our employees throughout the United States to have the resources and the organization to do their jobs. By working together with this Committee and the Congress as a whole we will make this happen.

Security for the homeland is a partnership. Not only must all of the elements of DHS work together toward a common goal, but DHS must also work in partnership with many other federal agencies, with State, tribal and local governments, with the private sector, and with ordinary citizens. In my prior positions I have worked closely with all stakeholders to ensure that we could accomplish our missions. If confirmed, I will continue on that path.

Within the federal government, the Department of Defense, the Department of Justice, the Department of Transportation, the Treasury Department, the Department of Agriculture, and the Environmental Protection Agency are just a few of the many cabinet level and independent agencies that have major contributions to make to keep our homeland secure. If confirmed, I will work to enhance the cooperation between the Department and other federal agencies.

Our state and local governments are of critical importance in protecting our citizens and assisting in any necessary recovery efforts. DHS has and will continue to work closely with the State and local governments to forge the necessary collaborative arrangements to focus our resources. I am sure that you were pleased to learn that Secretary Ridge just announced another round of grants to the States for the Urban Area Security Initiative (UASI). These awards made $725 million available for various critical urban security needs and they complement the almost $800 million that the Department's Office of Domestic Preparedness distributed during the previous fiscal year. The UASI is just one of the many grant programs run either by ODP or other elements of DHS to get needed funds into the hands of our elected State and local officials to fulfill critical homeland security needs, not the least of which includes first responders. One of the contributions I hope to make is to design accountability systems to help us recognize best practices and the general return realized from grant investments. The gravity and high stakes of our work demands that we get security return for the granted dollars.

Cooperation with the private sector is also of critical import. The private sector is, of course, the lifeblood of our economy. We must continue to enhance our security through commonsense measures that are effective, while at the same time allowing our industries to remain competitive in the global marketplace. This is a delicate balance. Many of our industrial centers are considered critical infrastructure, and the owners must be made aware of both their security vulnerabilities, and their responsibilities to help raise the security bar. The Department's Directorate of Information Analysis and Infrastructure Protection is charged with the mission to assess the vulnerabilities of this critical infrastructure and if confirmed I will support this vital mission.

DHS must also rely upon the private sector for much of the goods and services we acquire. Our contractors and their sub-contractors are part of our extended workforce. This includes critical information technology needed to gather and exchange intelligence information, and to allow almost 200,000 employees to operate in a modern networked environment. We also need the inventiveness of American industry and academia to develop and bring to market new technologies that enable us to do our job more quickly, at less cost, and more accurately. Our Science and Technology Directorate has that mission to look over the horizon to the allow us to face current threats as well as emerging threats. Through such innovative organizations as the Homeland Security Advanced Research Projects Agency, DHS will serve as an incubator of new security technologies. During my current assignment as Administrator of TSA I worked closely with Dr. McQueary and Dr. Albright on security technology related to transportation security. If confirmed I look forward to working with them on the broader science and technology issues that concern the Department.

Finally, defending the homeland is an opportunity and an obligation for all of our citizens. Whether it is being alert to unusual events in their neighborhood that may give rise to important intelligence information about suspected terrorist activity, or patiently waiting at an airport security checkpoint, each citizen can contribute to protecting our country, our people, and our homes. The events of 9/11 show that terrorists do not draw a distinction between military targets and civilian office buildings. Nor do they distinguish between ordinary citizens and members of our Armed Forces. Each of us is a target. Therefore, each of us must respond to the challenge.

I am very aware of the grave importance of the opportunity and the challenge that President Bush and Secretary Ridge have presented to me. While I am humbled by their faith in me and the awesome task that awaits me, if confirmed, I am confident that my more than 40 years in service to America have prepared me for this challenge.

I look forward to answering your questions.

BIOGRAPHICAL AND FINANCIAL INFORMATION REQUESTED OF NOMINEES

A. BIOGRAPHICAL INFORMATION

1. **Name:** (Include any former names used.)

James Milton Loy

2. **Position to which nominated:**

Deputy Secretary of Homeland Security

3. **Date of nomination:**

Announced by White House October 23, 2003

4. **Address:** (List current place of residence and office addresses.)

Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 22202

5. **Date and place of birth:**

August 10, 1942, Altoona, Pennsylvania

6. **Marital status:** (Include maiden name of wife or husband's name.)

Married
Kay Ann (McGirk) Loy

7. **Names and ages of children:**

Kelly Loy Morf (37)
Michael S. Loy (33)

8. **Education:** List secondary and higher education institutions, dates attended, degree received and date degree granted.

SCHOOL	ATTENDED	DEGREE	DATE
Altoona High School	1958-1960	Diploma	June 1960
U.S. Coast Guard Academy	1960-1964	BS	3 June 1964
Wesleyan University	1969-1970	MALS	June 1970
University of Rhode Island	1972-1974	MPA	May 1974
Industrial College Armed Forces	1984-1985	Graduate	June 1985

9. **Employment record:** List all jobs held since college, including the title or description of job, name of employer, location of work, and dates of employment. (Please use separate attachment, if necessary.)

TITLE	EMPLOYER	LOCATION	DATE
Deck Watch Officer	USCG	CGC ABSECON Norfolk, Va	1964-1965
Commanding Officer	USCG	CGC CAPE FALCON Little Creek, Va	1965-1966
Commanding Officer	USCG	CGC PT LOMAS Danang/Vung Tau Vietnam	1966-1967
Staff Officer	USCG	CG Headquarters (G-OS) Washington, DC	1967-1969
Student	USCG	Wesleyan University Middletown, CT	1969-1970
Instructor/Associate Dean	USCG	USCG Academy New London, CT	1970-1974
Executive Officer	USCG	CGC COURAGEOUS Cape Canaveral, FL	1974-1976
School Chief	USCG	Officer Candidate School Yorktown, VA	1976-1979
Commanding Officer	USCG	CGC VALIANT Galveston, TX	1979-1981
Branch Chief/Asst Div Ch.	USCG	CG Headquarters (G-PO) Washington, DC	1981-1984
Student	USCG	Industrial College of the Armed Forces Washington, DC	1984-1985
Commanding Officer	USCG	CGC MIDGETT Alameda, CA	1985-1986
EA to the Commandant	USCG	CG Headquarters (G-C-10) Washington, DC	1986-1989
Chief, Operations Division	USCG	CG Atlantic Area New York, NY	1989-1990

Commander	USCG	Eighth Coast Guard District New Orleans, LA	1990-1992
Chief, Personnel & Training	USCG	CG Headquarters (G-P) Washington, DC	1992-1994
Commander	USCG	CG Atlantic Area New York, NY	1994-1996
Chief of Staff	USCG	CG Headquarters (G-CCS) Washington, DC	1996-1998
Commandant	USCG	CG Headquarters (G-C) Washington, DC	1998-2002
Administrator	TSA	Dept of Homeland Security	2002-Present
Teacher: Public Administration Courses (Stationed at Training Center Yorktown, VA)		St. Leo's College Golden State University	1976-1979

10. **Government experience:** List any advisory, consultative, honorary or other part-time service or positions with federal, State, or local governments, other than those listed above.

None

11. **Business relationships:** List all positions currently or formerly held as an officer, director, trustee, partner, proprietor, agent, representative, or consultant of any corporation, company, firm, partnership, or other business enterprise, educational or other institution.

Director, Navy Mutual Aid Association	1992-1994
Director, National Capital Area Council, Boy Scouts of America	1996-Present
Honorary Director, Coast Guard Foundation	2002-Present

12. **Memberships:** List all memberships and offices currently or formerly held in professional, business, fraternal, scholarly, civic, public, charitable and other organizations.

Member, Council of Foreign Relations
Member, U.S. Coast Guard Academy Alumni Association
Member, National Naval Officers Association
Member, Naval Institute
Member, Coast Guard Combat Veterans Association
Member, Veterans of Foreign Wars
Member, Navy League of the United States
Member, U.S. Naval Order
Ex Officio, National Defense Transportation Association

13. **Political affiliations and activities:**

(1) List all offices with a political party which you have held or any public office for which you have been a candidate.

None

(2) List all memberships and offices held in and services rendered to all political parties or election committees during the last 10 years.

None

(3) Itemize all political contributions to any individual, campaign organization, political party, political action committee, or similar entity of $50 or more for the past 5 years.

None

14. **Honors and awards:** List all scholarships, fellowships, honorary degrees, honorary society memberships, military medals and any other special recognitions for outstanding service or achievements.

Honorary Doctor of Laws, Massachusetts State Maritime Academy
Honorary Doctor of Science, Webb Institute

2003 Naval Order of the U.S. Distinguished Sea Services Award
2003 Hudson Institute & USMMA Maritime Security Lifetime Achievement Award
2002 National Cargo Security Council National Leadership Award
2002 Seaman's Church Institute Silver Bell Award
2002 Reserve Officer Association's Minute Man Hall of Fame
2002 U.S. Navy League Admiral Arleigh Burke Leadership Award
2001 American Society of Public Administration/Government Executive Leadership
2001 Award Soldier's, Sailor's, Marine's and Airmen's Club Military Leadership Award
2000 NAACP Meritorious Service Award
2000 SEATRADE Personality of the Year

Military Awards:

Transportation Distinguished Service Medal (2)
Department of Defense Distinguished Service Medal
US Coast Guard Distinguished Service Medal (4)
Defense Superior Service Medal
Legion of Merit (2)
Meritorious Service Medal
Bronze Star (Combat 'V' Device)

CG Commendation Medal (5)
CG Achievement Medal
Combat Action Ribbon
Vietnam Campaign Medal
Republic of Vietnam Service Medal
Expert Pistol/Expert Rifle
Humanitarian Service Medal (2)
Numerous Campaign and Service Ribbons

15. **Published writings:** List the titles, publishers, and dates of books, articles, reports, or other published materials which you have written.
"The Versus Atmosphere" – US Coast Guard Academy Alumni Bulletin – 1978
"Exporting Coast Guard Expertise" (w/ CAPT B. Stubbs) – Naval Institute Proceedings – June 1997
"Leadership Development" – Naval Chaplain – June 1994
Diversity Comes of Age – Commandant's Bulletin – November 1993
"Meeting the Homeland Security Challenge: A Principled Approach for a Balanced and Practical Response" (w/ CAPT B. Ross) - Journal of Homeland Security, ANSER Institute for Homeland Security - September 2001 *(Attached)*
"Global Trade: America's Achilles' Heel" (w/ CAPT B. Ross) - Defense Horizons, National Defense University, No. 7, published concurrently in Journal of Homeland Security, ANSER Institute for Homeland Security - February 2002 *(Attached)*
"Protecting America's Borders" (w/ CAPT B. Ross), limited distribution paper prepared for the Homeland Security 2005 Conference - ANSER Institute for Homeland Security - May 2002 (now being revised as a chapter in an upcoming book)
"Character in Action: The Coast Guard on Leadership" (Co-authored w/ Don Phillips) - 2003

16. **Speeches:** Provide the Committee with four copies of any formal speeches you have delivered during the last 5 years, which you have copies of and are on topics relevant to the position for which you have been nominated.

Attached

17. **Selection:**

(1) Do you know why you were chosen for this nomination by the President?

I believe a skill set match was observed by the Secretary and the President that matched the challenge represented at DHS. My strengths lie in leadership of large organizations. I believe in strategic planning, visionary thinking, accountability, and performance based management. I was able to make those things happen at the Coast Guard during my tenure as Commandant and as well laid the groundwork at TSA. I am a conscious steward of the taxpayers' investment in programs. I am a proven crisis manager, both operationally and in the budget and policy battles inside the Beltway. I would apply those skills to developing DHS as

an efficient organization and a culture dominated by sound core values and a commitment to service.

(2) What do you believe in your background or employment experience affirmatively qualifies you for this particular appointment?

Throughout my public service career, I acquired extensive leadership skills and competencies. I view myself as a consensus builder with focus on developing private-public partnerships as well as a positive network with key impact players in the Administration and Congress as they are engaged in shaping DHS's future.

B. FUTURE EMPLOYMENT RELATIONSHIPS

1. Will you sever all connections with your present employers, business firms, business associations or business organizations if you are confirmed by the Senate?

   N/A

2. Do you have any plans, commitments or agreements to pursue outside employment, with or without compensation, during your service with the government? If so, explain.

   None

3. Do you have any plans, commitments or agreements after completing government service to resume employment, affiliation or practice with your previous employer, business firm, association or organization?

   None

4. Has anybody made a commitment to employ your services in any capacity after you leave government service?

   No

5. If confirmed, do you expect to serve out your full term or until the next Presidential election, whichever is applicable?

   Yes

C. POTENTIAL CONFLICTS OF INTEREST

1. Describe any business relationship, dealing or financial transaction which you have had during the last 10 years, whether for yourself, on behalf of a client, or acting as an agent, that could in any way constitute or result in a possible conflict of interest in the position to which you have been nominated.

   None

2. Describe any activity during the past 10 years in which you have engaged for the purpose of directly or indirectly influencing the passage, defeat or modification of any legislation or affecting the administration and execution of law or public policy other than while in a federal government capacity.

   - Field hearing testimony relative to counter-narcotics activities of the Coast Guard. Congressman Dennis Hastert chaired hearing in San Juan, Puerto Rico (1999).

   - Annual Authorizing and Appropriation hearings as Commandant of USCG and as TSA Administrator, from 1998-Present.

   - Meetings within Executive Branch and with legislative members regarding Coast Guard and TSA issues and missions.

3. Do you agree to have written opinions provided to the Committee by the designated agency ethics officer of the agency to which you are nominated and by the Office of Government Ethics concerning potential conflicts of interest or any legal impediments to your serving in this position?

   Yes

D. LEGAL MATTERS

1. Have you ever been disciplined or cited for a breach of ethics for unprofessional conduct by, or been the subject of a complaint to any court, administrative agency, professional association, disciplinary committee, or other professional group? If so, provide details.

   No

2. To your knowledge, have you ever been investigated, arrested, charged or convicted (including pleas of guilty or nolo contendere) by any federal, State, or other law enforcement authority for violation of any federal, State, county or municipal law, other than a minor traffic offense? If so, provide details.

No

3. Have you or any business of which you are or were an officer, director or owner ever been involved as a party in interest in any administrative agency proceeding or civil litigation? If so, provide details.

No

4. Please advise the Committee of any additional information, favorable or unfavorable, which you feel should be considered in connection with your nomination.

None

E. FINANCIAL DATA

All information requested under this heading must be provided for yourself, your spouse, and your dependents. (This information will not be published in the record of the hearing on your nomination, but it will be retained in the Committee's files and will be available for public inspection.)

AFFIDAVIT

James M. Loy being duly sworn, hereby states that he/she has read and signed the foregoing Statement on Biographical and Financial Information and that the information provided therein is, to the best of his/her knowledge, current, accurate, and complete.

James M Loy

Subscribed and sworn before me this 31st day of October, 20 03

Jeanette M. Bonaccorsy

Notary Public
My Commission Expires November 30, 2003

November 12, 2003

The Honorable Susan M. Collins
Chair
Committee on Governmental Affairs
United States Senate
Washington, DC 20510-6250

Dear Madam Chair:

In accordance with the Ethics in Government Act of 1978, I enclose a copy of the financial disclosure report filed by James M. Loy, who has been nominated by President Bush for the position of Deputy Secretary, Department of Homeland Security.

We have reviewed the report and have also obtained advice from the Department of Homeland Security concerning any possible conflict in light of its functions and the nominee's proposed duties. Also enclosed is a letter dated November 4, 2003, from Mr. Loy to the Department's ethics official, outlining the steps he will take to avoid conflicts of interest. Unless a specific date has been agreed to, the nominee must fully comply within three months of his confirmation date with the actions he agreed to take in his ethics agreement.

Based thereon, we believe that Mr. Loy is in compliance with applicable laws and regulations governing conflicts of interest.

Sincerely,

Amy L. Comstock
Director

Enclosures

U.S. Senate Committee on Governmental Affairs
Pre-hearing Questionnaire
For the Nomination of James M. Loy to be
Deputy Secretary of the Department of Homeland Security

I. Nomination Process and Conflicts of Interest

1. Were any conditions, expressed or implied, attached to your nomination? If so, please explain.

   Answer: No.

2. Have you made any commitments with respect to the policies and principles you will attempt to implement as Deputy Secretary of the Department of Homeland Security (DHS or Department)? If so, what are they and to whom have the commitments been made?

   Answer: I have made no commitments other than to be open to all inputs and synthesize those inputs as influences on policy or principles with the security of America as the goal. I believe it is important to do a good job interpreting the National Strategy for Homeland Security for the DHS workforce so they all feel confident that their work is channeled to the right ends. Although there are an endless list of opinions offered daily, my pledge is to work with the President, Secretary Ridge and the Congress to build the best security system for our homeland.

3. If confirmed, are there any issues from which you may have to recuse or disqualify yourself because of a conflict of interest or the appearance of a conflict of interest? If so, please explain what procedures you will use to carry out such a recusal or disqualification.

   Answer: I hold bonds issued by several States. I acknowledge that the broad mission of DHS may well have an economic impact on public facilities in the States. I am actively considering selling these assets. Today, the value of each of my bond holdings falls below the regulatory de minimus exception. In discussing this matter with the Departmental Designated Agency Ethics Official, until and unless I sell these assets, as provided in my ethics agreement, I will monitor the value of my bond holdings to ensure that their values remain within the exemptions.

II. Role and Responsibilities of the Deputy Secretary of Homeland Security

4. How do you view the role of the Deputy Secretary of Homeland Security? What would you highlight from your background and experience that will enhance your effectiveness in this role?

Answer: Classically the Deputy Secretary serves the Secretary. I will endeavor to do that faithfully. The Deputy must also be ready to substitute for the Secretary when required. I have spent the last six years in two significant positions ... Commandant of the U. S. Coast Guard and Administrator of the Transportation Security Administration. Both assignments were exceptionally demanding in the areas of strategic planning, mission focus, infrastructure and culture development. Those experiences, which required interaction with other administration colleagues, Members of Congress and their staffs, the media, academia, etc., have been good proving grounds for this position.

5. What do you expect the role of the Deputy Secretary will be in relation to the Secretary and his statutory responsibilities?

Answer: The Deputy Secretary will likely be expected to run the day-to-day activities for the Secretary, and be an advisor and alter ego as necessary. The Secretary's statutory responsibilities are exclusively his and the Deputy must be ready to stand in to those responsibilities as required.

6. What would be your priorities as Deputy Secretary?

Answer: My priorities will be to contribute to the ongoing effort to stand up this enormous department and to merge the 22 agencies that joined on 1 March 2003 into an efficient and effective organization. DHS has the opportunity to build the model cabinet agency for the 21st Century. All the support functions can be designed to optimal standards. The operating agencies can be merged to the optimal service delivery required in a new, post 9/11/01 security environment. Those are huge tasks that MUST be done well for the sake of the country. Our priorities must be mission accomplishment, functional design, process design and infrastructure organization to meet the challenge.

III. Policy Questions

Transition and Reorganization Planning

7. The HSA requires DHS to ensure that agency functions not directly related to homeland security are not diminished or neglected. Some have expressed concerns that non-homeland security missions over time may not receive adequate funding, attention, visibility, and support within the Department. What will you do as Deputy Secretary to ensure that proper attention is given to non-homeland security missions?

Answer: We recognize that many elements of the Department such as FEMA, the Secret Service and the Coast Guard have critical missions in addition to their specific homeland security responsibilities. As such, I will meet frequently with Departmental leadership to ensure that we are carrying out all of our missions to the best of our ability.

We understand that our responsibility to the Congress and the taxpayer includes ensuring that both our homeland security and non-homeland security missions are adequately

resourced and carried out. Our FY 2004 budget acknowledges our non-homeland security missions and requests that the Congress provide resources to ensure that those missions are fully discharged. Our Congressional justifications elaborate on these missions and responsibilities.

The Department is currently setting up formal mechanisms and measures to monitor the performance of all of its activities, including non-homeland security activities. As required by the Government Performance and Results Act, the Department will publish performance measures for its activities in its first annual Performance Report in February 2004 and as part of its FY 2005 Annual Performance Plan. The Department will use the results of the performance measures to help determine resource requirements.

Strategic Planning and Reporting

8. The Government Performance and Results Act (GPRA) provides a framework for federal agencies to achieve greater program and operational accountability. There has been ongoing difficulty with many federal agencies setting adequate performance goals, objectives, and targets.

- What specific direction and criteria are DHS managers provided regarding setting performance goals and measures?

Answer: GPRA is designed to ensure programs are held accountable for achieving results by setting program goals, measuring program performance, and reporting publicly on their progress. Its drive is to increase program efficiency and effectiveness and help departments and agencies improve program management, resource allocation, and accountability. A key requirement under GPRA is a departmental strategic plan that is the basis for establishing annual performance measures tied to the budget.

The Department is currently preparing its strategic plan that will include departmental goals, objectives, and strategies. The Department's Strategic Plan will provide focused guidance for DHS managers to establish supporting goals, objectives, and strategies to accomplish the Department's mission. The strategic plan also will provide the standards for accurate and concise measurement of agency performance. The Department's FY05 budget request will provide annual performance measures.

The CFO's Office issued performance measures guidelines in conjunction with its review of performance measures in June/July 2003. Refinement and improvement of performance measures is an ongoing and integral part of the DHS annual Planning, Programming, and Budgeting System (PPBS).

- How does DHS go about setting strategic and annual performance goals?

Answer: The Department is currently preparing its Strategic Plan including departmental and organizational elements goals, objectives, and strategies. The Department's Strategic Plan and additional planning guidance will provide focused

guidance for departmental objectives and provide the standards for accurate and concise measurement of agency performance.

The Strategic Plan will be the cornerstone for the Department's long-term comprehensive program review system—the Planning, Programming and Budgeting System (PPBS). We will align resources to programs that support DHS missions, demonstrate accountability, are performance driven, have identified long-term benefits, and meet the Department's priorities. The PPBS will provide the framework for developing the Department's Future Years Homeland Security Program (FYHSP) (required by the 2002 Homeland Security Act). The FYHSP will define programs and associated resource allocations, or budgets, five years beyond the upcoming budget year.

- Annually, the Department will issue planning guidance (based on the Strategic Plan) that will be the roadmap for the Department's resource planning and program evaluations.

- DHS agencies will develop proposed programs consistent with the planning guidance and the Department's strategic plan. These programs will reflect systematic analysis of missions and objectives to be achieved, alternative methods of accomplishing them, and the effective allocation of resources to accomplish the objectives.

- The FYHSP will be foundation of the budget. All programs within the FYHSP and, therefore, the budget will directly support the Department's Strategic Plan.

- What planning consultation should DHS do internally and externally?

Answer: The Department is currently preparing its Strategic Plan including departmental and organizational elements goals, objectives, and strategies. The Department's Strategic Plan and additional planning guidance will provide focused guidance for departmental objectives and provide the standards for accurate and concise measurement of agency performance.

The Strategic Plan will be the cornerstone for the Department's long-term comprehensive program review system—the Planning, Programming and Budgeting System (PPBS). We will align resources to programs that support DHS missions, demonstrate accountability, are performance driven, have identified long-term benefits, and meet the Department's priorities. The PPBS will provide the framework for developing the Departments Future Years Homeland Security Program (FYHSP) (required by the 2002 Homeland Security Act). The FYHSP will define programs and associated resource allocations, or budgets, five years beyond the upcoming budget year.

- Annually, the Department will issue planning guidance (based on the Strategic Plan) that will be the roadmap for the Department's resource planning and program evaluations.

- DHS agencies will develop proposed programs consistent with the planning guidance and the Department's strategic plan. These programs will reflect systematic analysis of missions and objectives to be achieved, alternative methods of accomplishing them, and the effective allocation of resources to accomplish the objectives.

- The FYHSP will be foundation of the budget. All programs within the FYHSP and, therefore, the budget will directly support the Department's Strategic Plan.

- How should DHS ensure that GPRA principles are implemented and sustained within DHS?

Answer: DHS is complying with GPRA requirements by practicing good stewardship of our resources and looking for more effective and efficient ways of doing business. Holding managers accountable for achieving established goals and results is integral to DHS's financial management and planning. The DHS Planning, Programming, and Budgeting System (PPBS) is being fully implemented for development of the DHS budget and FYHSP. This process has the GPRA principles of performance based planning, budgeting and reporting embedded in the system.

Additionally, as required by GPRA, DHS will prepare and submit to Congress its annual plan and performance report. These documents will provide visibility and accountability to Department programs and operations.

Each annual budget request starting in FY05 will also include our performance plan, linked directly to the strategic plan and showing the associated planned resource levels. The FY05 budget itself will identify performance measures and planned outcomes related directly to our request for resources.

9. The Director of the Office of Management and Budget (OMB) has indicated that federal agencies—especially those agencies with homeland security missions—can expect increased oversight and more pressure to demonstrate performance in order to receive funding increases.

- What, if any, risks might there be associated with linking funding for homeland security activities directly to agency performance?

Answer: A risk of linking funding directly to agency performance could be that under-performing programs could face budget cuts before the reasons for poor performance are fully recognized and understood. Poor performance may be due to uncontrollable external factors even when programs are doing the right things.

However, an agency's budget request should directly link to performance. Both the Congress and the American public should hold the Department and the senior managers

responsible for meeting established performance targets and delivering measurable value to our Nation.

The Department's goal is to have a fully integrated budget planning and program performance system (the Future Years Homeland Security Program (FYHSP), that aligns resources to programs that meet the Department's priorities, support our objectives, demonstrate accountability, are performance driven, and have identified long term benefits. Our first strategic plan will be the cornerstone of the Future Years Homeland Security Plan, and will be the roadmap for resource planning and program evaluations. We will link performance goals with resource allocation plans to form the foundation of the budget.

The Department's investment review process is in place to ensure program cost, schedule, and performance accountability measures are in place and enforced, that programs are not duplicative to others in the Department, and that all major programs support the Department's goals and objectives.

DHS is in the process of establishing FYHSP programmatic reviews to integrate Departmental priorities, and DHS has established resource planning, investment control, budgeting, acquisition, and investment management. This will ensure resources are wisely used and spending directly supports and furthers DHS's mission and provides optimal benefits and capabilities to stakeholders and customers.

It will also allow us to identify poorly performing programs and investments so corrective actions can be taken.

- What specific steps have been taken or should be taken to hold DHS executives accountable for performance?

Answer: An agency's budget request should directly link to performance. Both the Congress and the American public should hold the Department and the senior managers responsible for meeting established performance targets and delivering measurable value to our Nation.

The DHS Planning Programming and Budgeting System will require agencies to report periodically to the CFO and Secretary progress on achieving program milestones established in the annual budget request to Congress.

The Department is using OMB Program Assessment Rating Tool (PART) to assess agency performance. The intent is to conduct PART reviews on all DHS programs. PART reviews are included as part of the Department's budget review process.

We are in the midst of a major project to establish measures-of-effectiveness for the Secretary's and agency-head's use in evaluating the success of the Department in achieving its objectives.

The DHS human resource system will include provisions that hold executives accountable for performance in their areas of responsibility.

We are establishing systems to collect and report performance information to support senior manager program performance reviews.

The Department's investment review process is in place to ensure program cost, schedule, and performance accountability measures are in place and enforced, that programs are not duplicative to others in the Department, and that all major programs support the Department's goals and objectives.

10. The creation of the Department of Homeland Security, which is now the third largest cabinet agency, is the largest governmental reorganization since the creation of the Department of Defense after World War II. The Department is merging 22 separate agencies with over 170,000 employees, and it must complete this merger while simultaneously strengthening our nation's day-to-day defenses against terrorist attacks and natural disasters. According to a recent report by the National Academy of Public Administration, the challenges of establishing and organizing the Department entail the "entire spectrum" of public management issues. These include: merging separate cultures, missions and systems, establishing effective communications, coordinating with Congress and other Departments, working collaboratively with state and local officials, setting overall priorities, and establishing an effective personnel system. Meeting these and other challenges require sustained and focused leadership throughout the Department.

- How would you assess DHS's record thus far in addressing the significant management challenges that it faces? In which areas have there been the most progress and in which areas has progress proven more problematic?

- What key lessons are you aware of from past governmental or corporate mergers and reorganizations and how do you believe they are applicable to the DHS?

Answer: We are fortunate to have in our leadership dedicated and visionary people with a wide range of experience in policy, operations, government at all levels, and the private sector. We draw on that breadth of experience in our efforts to create this new Department.

DHS has also involved our senior leadership in understanding the experience of the private sector in undertaking large mergers.

A key lesson is that communication is paramount. Change is unsettling, and leadership must explain that change to personnel clearly, concisely, and frequently. Personnel must be treated with courtesy, respect, and compassion. Second, steps toward integration must be carefully thought out and then executed quickly and smartly to minimize disruption and uncertainty.

Third, personnel need an opportunity to communicate back to leadership on their concerns and their insights. These individuals are the backbone of the Department, the operators, and the changes that are to be made are intended to increase their ability to do their jobs.

We have made numerous changes already, most notably in the Bureau of Transportation Security, where we have integrated components from various Agencies and Departments. I would give us high marks in our efforts here.

Financial Management

11. With the exception of the Department of Homeland Security, all Cabinet-level departments in the government are required to comply with the financial management and reporting requirements of the Chief Financial Officers Act of 1990. The Department is voluntarily complying with Act's requirements, including producing annual audited financial statements, but is not statutorily required to do so.

Do you support legislation, which has been approved by this Committee, to make the Department of Homeland Security subject to the financial management requirements of the CFO Act?

Answer: I applaud the spirit with which S. 1567, "Department of Homeland Security Financial Accountability Act", was introduced and agree that increased accountability is important and necessary. While I concur with the overarching goals that S. 1567 seeks to accomplish, I believe that legislation may not be necessary. The Department complies with the provisions of the Chief Financial Officers Action of 1990 and will continue to do so. The proposed legislation will not change the Department's requirements the Department must comply with in accounting for its finances. Also, the Department is subject to the oversight of the Office of Management and Budget, the Department's Office of Inspector General, and the General Accounting Office to ensure that the Department complies with federal financial management laws and regulations.

Acquisition Management

12. DHS has been faced with the challenge of integrating the procurement functions of 22 transferred agencies. Each legacy procurement office had its own procedures and policies and ways of doing business.

- How has DHS handled the task of integrating the various procurement organizations?

Answer: The Chief Procurement Officer (CPO) has taken charge of the procurement function in the Department. The CPO coordinates with the acquisition leadership in developing the DHS strategy for procurement. DHS is publishing a single Departmental acquisition regulation. This will be published in the Federal Register effective in December 2003. The regulation will provide uniform governing rules, policies and

guidance for the contracting offices within the Department. Finally, DHS has created a robust investment review process for acquisitions that are valued at $100,000 or greater. This process is described in detail below.

- Should DHS centralize the procurement function across DHS, or should each constituent organization handle its own procurements?

Answer: One of the founding tenets when forming the Department was to integrate redundant activities. We are currently studying a variety of strategies to gain administrative efficiencies.

- What more can DHS' centralized procurement office do to ensure the various procurement shops follow uniform standards to maximize benefits from economies of scale?

Answer: DHS has a variety of initiatives underway to promote uniform standards and economies of scale:

1. Investment Review Board (IRB) – The IRB process integrates planning, controls, budgeting, acquisition, and management of investments to ensure public resources are wisely invested. This process was developed for two primary purposes; to ensure DHS senior management is aware of and approves major investments through systematic reviews at key decision points in the acquisition life-cycle and to identify duplicative efforts for possible consolidation to achieve economies of scale can. Thresholds for review begin at $100,000 for information technology investments and are incrementally increased depending on complexity and risk. The Deputy Secretary chairs the IRB.
2. To further support the IRB process, DHS established a strategic sourcing initiative focused on creating departmental strategies for acquiring goods and services of strategic importance to the Department. This process supports the DHS Investment Review Process with the ultimate objective of consolidating requirements whenever feasible to achieve efficiencies and economies of scale.
3. DHS is developing a more consistent acquisition workforce training program to promote consistency, uniformity, and portability for our acquisition professionals
4. As discussed previously, DHS is finalizing its acquisition regulation supplement and manual to create standard processes throughout the Department.
5. The DHS procurement function is working closely with the Office of the Chief Financial Officer, who is creating a unified process and set of systems for finance, accounting, procurement and asset management. A migration to a unified system and process will assure uniformity.

13. In the HSA, Congress provided DHS with a range of new authorities to acquire goods and services in a streamlined manner. In other federal agencies, GAO has raised issues about cost and schedule overruns, inadequate oversight of contracts, and an inability to hold contractors accountable. In exercising the provided procurement flexibility, DHS

needs the right internal controls to ensure that its streamlined procurements address DHS' true needs.

- What has DHS put in place to ensure strong systems and controls for acquisition?

- What additional steps should DHS plan to create a strong DHS capability to oversee and manage contractors?

Answer: In addition to the efforts outlined above, DHS has adopted the GAO framework for improving the procurement function. This framework is designed to enable senior agency officials and accountability organizations to conduct high-level, qualitative assessments of an agency's procurement processes.

With respect to oversight and management of contractors, DGS has established agreements with the Defense Contract Audit and Administrative agencies to provide supplementary contract audit and administrative support. We have also established training requirements for our Contracting Officer Representatives (COR) and Program and project management staff to strengthen oversight and management of contractor performance. Finally, the use of performance based service contracting as a standard practice within DHS requires the use of measurable contractor performance standards, which allow for contract deductions when specific performance standards are not met.

Competitive Sourcing

15. In furtherance of the Administration's competitive sourcing agenda, the DHS announced in August that it would be subjecting the jobs of more than 1,100 immigration information officers (IIO's) to a competition with private contractors. The Department acknowledged that the IIO's perform adjudicatory functions and that their work is critical to the nation's security.

Answer: The decision to study these positions was made by the Department of Justice, and DHS inherited it, just as DHS inherited other studies that were underway at the Coast Guard. DHS decided not to reverse the decisions made on these studies by other Departments and Agencies. Many activities that are critical are performed by the private sector. In fact, we have private sector employees working in Iraq, some of whom recently lost their lives in this effort. As this example shows, even high-risk dangerous jobs necessary for national security can be and are undertaken by private contractors. Whether jobs might be competed is not based on their importance, but on whether they are commercial in nature, that is, whether the private sector can also perform them.

- What will be the effect of this competition on employee morale?

Answer: The first thing to note is that the government wins these competitions in the vast majority of cases. Such competitions can produce feelings of unease in employees, particularly if senior management isn't aggressively doing its job of communicating and

explaining what the competitions are about and why they're being undertaken. When senior management does do its job, however, employees' concerns are minimized, morale is maintained, and work is accomplished.

- Does DHS have sufficient trained staff to adequately conduct and oversee the competition? Why has the Department retained several different consulting firms to assist with the competition?

Answer: It is my understanding that we have sufficient staff to oversee the competition. Most, if not all, Departments and agencies retain contractor support for data gathering and analysis. Contractors do not make decisions on policy-related matters, however.

- What do you believe are the benefits of conducting this and similar competitions? What do you believe are the costs?

Answer: The data show that on average – even when the government wins the competition – the taxpayer saves 25% of the operating costs. In some cases, the savings are much higher. This is a significant benefit. The costs vary, depending on the complexity of the study, but can range from $3000 - $5000 per position studied, depending on the circumstances.

16. OMB Director Joshua Bolten told the Committee that he was committed to providing opportunities for federal employees to compete for new work, and for work currently performed by private contractors. Will DHS provide federal employees with opportunities to compete for new work, and for work currently performed by contractors? If so, what specific initiatives will DHS undertake to identify such work and open it to competition?

Answer: DHS has just completed its FAIR Act inventory. [NB: this was just approved by OMB and will ultimately be published.] Of the positions deemed eligible for competition, the Department has not yet determined which if any should be studied. There are instances in which work performed by contractors has been brought back in-house [the Department of Energy brought security positions in-house last year, for example]. I would expect that DHS would look at such opportunities as well.

Information Technology Management

17. Geospatial information is an enterprise asset because it cuts across all business functions. Within DHS specifically, geospatial information is used for intelligence analysis, critical infrastructure protection, enforcement, border security, first responders, disaster recovery, management, and facility construction and planning. These functions are managed by multiple offices within the Department and utilize different geospatial programs, techniques, and processes. Each has different priorities, goals, and values. However, this decentralized approach is resulting in inadequate geospatial data compatibility, insufficient geospatial data sharing, a lack of geospatial technology interoperability,

inefficient geospatial data collection, and institutional and organizational resistance. Senator Allard has introduced a bill that would give the Department's Chief Information Officer the responsibility of managing the geospatial needs of the Department and overseeing implementation of geospatial standards.

Do you support giving the Department's Chief Information Officer these responsibilities?

Answer: Geospatial data compatibility extends far beyond the bounds of the Department. Thus, the Secretary and his designees have the responsibility to create partnerships both within the Department and with other federal agencies and state and local governments. The role of the Chief Information Officer's Office is threefold: it is responsible for establishing an architecture for DHS information systems; maintaining those systems to provide an accepted or agreed-upon level of service; and managing the process through which new information technologies or systems are introduced into and integrated with the Department's information infrastructure. Identifying new information technologies and the subsequent design and development of systems using them is the province of the Science and Technology Directorate who has the responsibility for Research, Development, Testing and Evaluation (RDT&E), and associated Standards for the Department. For example, the Information Analysis and Infrastructure Protection and Science and Technology Directorates recently met a critical need for geospatial information integration for the Department.

It is my understanding that the department is working internally to address the coordination of geospatial information and technologies at present. While the Chief Information Officer has an important leadership role to play with regard to the tools, techniques, technical standards used within the department, data and technology interoperability, and software and hardware deployed and used to support geospatial activities, I believe that the Secretary should be given the discretion to determine how best to address the geospatial arena within the department.

18. How should information security be built into the Department's IT systems? Should there be requirements that commercial off-the-shelf software purchased by the Department includes adequate information security? If so, what standards should be used to implement such a policy?

Answer: In order to ensure that information security is built into the Department's IT systems the Department of Homeland Security has implemented a comprehensive Information Security program that is fully aligned with the direction provided in the Federal Information Security Management Act of 2002 (FISMA). The Department's Security Program specifically addresses eight program areas including; Program Management and Integration, Security Policy, Compliance and Oversight, Security Training and Awareness, Security Architecture, Security Operations, Continuity Planning, and National Security Systems and Communications Security.

Integral to the overall Information Security Program, the use of evaluated and endorsed commercial-off-the-shelf products is encouraged by giving preference to those products

that have completed Common Criteria certification through the National Information Assurance Partnership, sponsored by the National Security Agency and the National Institute of Standards and Technology. While this provides a robust catalogue of security profiles, it is anticipated that in the future the Department will also be providing new mission specific profiles based on unique Department requirements.

19. Many agencies with a vital role in the homeland security mission remain outside of the new Department. These include the FBI and CIA, the State Department, and state and local governments. It is essential in the war against terrorism that these agencies and others are able to share data and communicate with each other and with the new Department of Homeland Security.

- What has been done thus far to ensure that the different agencies and levels of government involved in homeland security are linked through an interoperable information system?

Answer: By creating the Department, the Congress took a great step toward bringing together many of the Federal agencies most involved in homeland security - - Customs, INS, Border Patrol, and others. We've put huge efforts into integrating these functions, both at the level of technology and at the level of operational processes. We're building a single DHS wide-area network, for example, and we've already got a common e-mail domain and Department-wide collaboration capabilities.

Immediately after the Department's formation last Spring, the key Federal agency partners laid the policy basis for information sharing in a Memorandum of Understanding that gives priority to preventing terrorism and mandates faster and broader exchange of law-enforcement and intelligence data. Additional MOUs and operating agreements implementing this policy have been developed around specific needs.

In May, the President established the Terrorist Threat Integration Center (TTIC), and DHS immediately assigned staff on site to coordinate information exchange, while technical staff has been working closely to establish secure communications for automated operations.

Following issuance of HSPD6, DHS, the FBI, the CIA and State Department established a framework for interagency cooperation to set up the Terrorist Screening Center for initial operations on December 1. DHS, FBI, and State Department staff are moving into this joint operations center right now, and establishing the secure communications and systems to create a consolidated Watch List for use by all key agencies. At the same time, the agencies are planning for a May 2004, milestone to further automate the distribution of these data by establishing direct system-to-system links, based on a common data format.

Agreed standards for data exchange are a key enabler for integrated computer systems. DHS is leveraging work already under way in the Department of Justice

through its GLOBAL Information Sharing Initiative and the Intelligence Community's Metadata Working Group. Our goal is maximum use of common data formats so that Federal and local partners can build systems that will immediately interoperate with others, without expensive customization.
We are working with major associations representing State and local technology leaders, like NASCIO, both to learn their needs and priorities and to let them know our plans. We also tap into this information via the established Justice GLOBAL Advisory Committee, of which our CIO is a member.

Our technology strategy emphasizes the use of public or widely implemented industry standards, so partners can build systems to these standards with confidence that they will work together.

In September, we published the first Homeland Security Enterprise Architecture to communicate our planned approach to all partners and to the vendor community as well. Recognizing the criticality of these plans, we produced them in record time and have already started on the next version.

- Which office has taken the lead in that effort thus far, the Office of Homeland Security or the Office of Management and Budget? What will be your role in this effort?

Answer: Improved interoperability for more effective sharing of homeland-security information is a core strategy for the Department: we are responsible for making that happen. That said, OMB is a close partner in that effort, and DHS has worked together closely on funding and policy issues in vital areas like the recently-announced Terrorist Screening Center for consolidating Watch Lists, and plans for interoperable wireless communications.

- What initiatives are planned for the future to ensure that the different agencies and levels of government involved in homeland security – including the component agencies of DHS -- are linked through an interoperable information system?

Answer: The next release of the Homeland Security Enterprise Architecture will include a framework for exchange of sensitive-but-unclassified information with all our partners via a common network and set of standards. DHS is coordinating with ongoing Justice work to make sure our many common partners in law enforcement and anti-terrorism have a clear and consistent framework for information exchange and system-to-system interoperability.

DHS is taking initial steps to create a Homeland Security Data Network (HSDN) that will provide CLASSIFIED connectivity and collaboration among DHS agencies and with our Federal, State and local partners. We are coordinating HSDN with key partners including Defense, the Intelligence Community and Justice.

Increased coordination of technology standards and plans with external partners, particularly non-Federal organizations, is a priority for the coming year, and DHS will continue to focus on public and broadly implemented industry standards, and actively promote standards in areas where they are missing.

DHS has initiated a data standardization program that will assure that new DHS systems will be able to exchange data with other systems inside and outside the Department. DHS is committed to coordination of these standards with the Intelligence Community, Justice, Department of Defense, and existing standards and practice in industry and local governments.

Human Capital Management

20. In a recent report on agency reorganization and modernization, GAO reported: "A successful merger and transformation must involve employees and their representatives from the beginning to gain their ownership for the changes that are occurring in the organization. Employee involvement strengthens the transformation process by including frontline perspectives and experiences." (Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations. July 2003. GAO-03-669.) GAO emphasized that timely, two-way communications between managers and employees is central to forming the "partnerships that are vital to the success of any organization." The appendix to the GAO report included an illustrative example from Deloitte & Touche. This example highlighted Deloitte & Touche's practice of "prereleasing" important information to employees offers the courtesy to employees of receiving information first" and enables feedback from employees so that senior management can address any concerns. Moreover, GAO advised that changes to the work environment are best developed collaboratively: "Major changes resulting from the merger can include redesigning work processes, changing work rules, developing new job descriptions, establishing new work hours, or making other changes to the immediate work environment that are of particular concern to employees. In leading organizations, management and employee representatives work collaboratively to gain ownership for these changes."

- Do you agree with GAO's views? If so, please explain how you believe such consultation and collaboration can help the Department of Homeland Security fulfill its mission.

Answer: I generally support GAO's views on the importance of consultation and collaboration in any organizational transformation – this is a belief that I have practiced throughout my career and particularly in my leadership roles in the U.S. Coast Guard and at the Transportation Security Administration.

The Department of Homeland Security can benefit from such participation in many ways by developing fundamental processes such as the Human Resource Management System where we have demonstrated our commitment to including employees and their representatives in the design of the new system; and by constantly learning from

employees how processes and procedures can be improved in a total quality environment such as the Coast Guard has applied at the Yard in Baltimore.

As GAO recognizes, organizational transformation is a process that takes many years – DHS, therefore, needs to continue to promote quality communication with employees throughout the building of the organization – we have done that with town hall meetings and focus groups not just on human resource issues but on operational decisions, ensuring that employees have the opportunity to provide feedback to senior management so that we can address their concerns.

- What consultation and collaboration with affected employees and their representatives did you engage in as you implemented the reorganizations involved in the creation of the TSA and its transition into DHS?

Answer: In its infancy TSA instituted several activities to ensure consultation and collaboration with employees and their representatives to facilitate a smooth stand-up of TSA and transition into DHS. Regarding the stand-up of TSA, two formal town hall meetings were held with employees from the Federal Aviation Administration's Office of Civil Aviation Security (ACS), which was merged with TSA. The Under Secretary provided a clear vision of the future of TSA, which would include the ACS employees. Open microphones were used to receive and respond to questions from the employees.

Once news of the establishment of the DHS was announced, TSA immediately began inform employees of the impact of the new Department on TSA. Broadcast email messages were used to deliver a consistent message. The TSA Intranet was also used. TSA detailed staff to DHS to provide support for the stand-up of the new Department, and to also keep TSA and it's employees informed of the latest transition activities. TSA's newsletter, *Sentinel,* was also used to keep employees informed the latest activities. As the transition began to proceed, a Town Hall meeting of all TSA employees was held. Questions from attendees were received and responded to. Many of the above described tools and activities continue to be used to keep all employees informed of DHS transition actions.

- What approach to such consultation and collaboration with employees and their representatives will you apply if you are confirmed as Deputy Secretary?

Answer: If I am confirmed as Deputy Secretary, I am committed to continuing to ensure open communications with employees at all levels of the organization – through town hall meeting and focus groups, through including employees in design teams and challenge sessions, and through working with employee representatives on matters of importance to them.

DHS has made a commitment to the union leaders that DHS will continue to involve them in the critical design of the human resource management system – one of the most important infrastructure challenges facing the Department. I would envision similar involvement in other endeavors whether at the Headquarters or local level.

Human Capital Management

21. Ensuring the civil rights of the 170,000 employees being transferred into the Department will be a critical challenge and will have a major effect on the morale of the employees charge with protecting our nation's homeland security.

- If you are confirmed as Deputy Secretary, how will you ensure that DHS develops into a model federal agency with respect to civil rights and anti-discrimination policies and performance?

- What has been your experience in addressing this issue at TSA and in the Coast Guard and what have been your major accomplishments?

Answer: Secretary Ridge and the senior leadership of the Department are fully committed to ensuring the civil rights of all employees within the Department. We believe that equal employment opportunity is a cornerstone for an effective workplace. On October 9, 2003, Secretary Ridge issued a memorandum to all Department employees stating his personal commitment to make the Department a model employer with a diverse and effective workforce. As Deputy Secretary, I plan to work closely with the Department's Human Capital Office and the Office for Civil Rights and Civil Liberties to ensure that the Secretary's commitment is completely fulfilled. I will also work closely with the equal employment opportunity and civil rights offices within the component agencies on these issues.

Both the Coast Guard and TSA have robust equal employment opportunity and civil rights offices. Throughout my career, I have been concerned about issues of fair employment and I will continue to place a priority on them.

22. The Department of Homeland Security Senior Review Advisory Committee recently met to discuss 52 options for the DHS personnel system. Despite the Federal Register notice's pledge that the Committee would determine which options should move forward to the Secretary and Director of the Office of Personnel Management, the Committee did not explicitly develop a set of recommendations for the Secretary and Director to consider. There were numerous issues on which the Committee did not reach agreement.

- Without guiding principles, and a tight timeframe, do you feel the Department, in conjunction with the Office of Personnel Management, will have time for the thoughtful evaluation required in establishing a new personnel system?

Answer: The Senior Review Committee adopted guiding principles against which the Secretary and the Director can evaluate the options. These principles are mission centered; performance focused; contemporary and excellent; generate respect and trust; and based on merit system principles and fairness.

The three-day public meeting of the Senior Review Committee on October 20-22 focused on these principles and helped to highlight elements and options that the Committee members believe should be considered by the Secretary.

Departmental senior staff, in conjunction with senior OPM staff, have been working since that SRC meeting to ensure that the new personnel system is established that best meets the guiding principles.

- How will the Department, in conjunction with OPM, ensure the new personnel system incorporates employee perspective and allows for validation by employees?

Answer: DHS is committed to continuing involvement of employees and their representatives in the design and validation of the human resource policies and procedures.

- What are the major management challenges in developing and implementing the new personnel system?

Answer: The major challenges include:
  - Creating an environment of trust with our employees and their representatives;
  - Ensuring continuous high quality communications with employees throughout the design and implementation of the system. DHS needs to set expectations for all employees so that they understand the new system and the improvements that will result from these changes;
  - Providing quality training for managers and supervisors who will be pivotal in ensuring that the system works; and
  - Ensuring that DHS funds the up-front investment of time and money required both to design the system, to communicate with our employees, and to train all the workforce on the new system rules.

- What will be the Department's approach to labor-management relations and systems for employee appeals? How will the Department ensure due process is afforded to employees? Will the Department guarantee employees subject to adverse actions the right to appeal to an independent third party?

Answer: Decisions regarding each of these issues have not yet been made. However, I can assure you that the Department is committed to continuing to build a strong, trusting relationship with the appropriate employee representatives. We will continue to involve those representatives in pre-decisional consultation and to bargain as appropriate.

A fundamental principle of the system that DHS adopts will be to assure due process for employees and to assure that their appeals are heard and decided in a fair and objective way.

- What style of arrangements involving labor and management do you intend to foster?

Answer: DHS has committed to a continuing role of the unions in the design of the human resource management system – and as part of that commitment to encouraging consultation with the appropriate representatives of DHS employees.

23. Will the new personnel system provide employees and their representatives access to independent third party review of negotiability determinations, bargaining impasses, unfair labor practice cases, arbitration cases, and bargaining unit determinations? If so, will the Department continue to rely on the Federal Labor Relations Authority and Federal Services Impasses Panel or will the Department establish alternative labor-relations bodies? If not, why not? Do you envision a process where the Secretary could suspend bargaining obligations for national security reasons? If yes, how will national security be defined?

Answer: Decisions regarding the role of the FLRA and FSIP have not yet been made. Many of the options developed by the Design Team and discussed at the Senior Review Committee meeting in late October included the authority for the Secretary to suspend bargaining obligations for national security reasons. DHS is still reviewing all the labor relations options.

24. What are your priorities and goals for changes in the personnel systems at DHS?

Answer: Our major goal is to create a new human resource management system that supports the critical mission of the Department -- a mission that has enormous consequences to our country and to every American citizen. It is abundantly evident that new realities clearly demand new solutions.

The system that we design must establish an environment of trust with our employees – a major component of that environment is ensuring continuous high quality communication with employees during the development of the system and throughout its implementation.

The Department has established the foundation for employee involvement during the design of the options being considered by the Secretary and the Director – in addition to the collaboration required by the HSA legislation as we publish regulations and make final decisions, DHS is committed to continuing to involve employees and their representatives in the more detailed design of the personnel policies and practices at DHS.

In a recent meeting with the presidents of the three major employee unions, the Secretary reiterated that commitment.

25. On January 9, 2003, you issued an order prohibiting federal baggage and passenger screeners from unionizing. You explained in a statement: "Fighting terrorism demands a flexible workforce that can rapidly respond to threats." You further stated: "That can

mean changes in work assignments and other conditions of employment that are not compatible with the duty to bargain with labor unions."

What specific findings did you make about the role and mission of the screeners that led you to conclude that collective bargaining would not be appropriate?

Answer: Ultimately, it is the responsibility of the leadership in every Department and agency to protect the merit principles and create a work environment where employees can effectively perform their duties. That responsibility can be enhanced by appropriate collective bargaining. Collective bargaining can also contribute to the effective conduct of public business.

26. The Department of Homeland Security contains a number of front-line inspection and security forces that now have collective bargaining rights, including:

- Customs and Border Protection
- Federal Protective Service
- U.S. Border Patrol

  - Do you believe the missions of these front-line inspection and security forces are incompatible with collective bargaining rights? If so, please explain.

Answer: We have been working closely with their union representatives on the design of the new human resource management system that includes a discussion of labor relations. I am pleased that all three unions (AFGE, NTEU, and NAAE) have recognized that there are situations when collective bargaining may need to be set aside to meet mission operations.

We are considering the union comments, along with those of the other Senior Review Committee (SRC) members, as we deliberate the final proposed rules.

27 On September 2, 2003, Secretary Ridge provided notice to Congress that the Federal Air Marshal program and Explosives Unit would be moved from TSA to the Bureau of Immigration and Customs Enforcement. What consultation did you and other top officials of the Department undertake with affected senior managers before the decision was made, and before the announcement was made, to undertake this reorganization? What consultation did you and other top officials of the Department undertake with other affected employees during those time periods? Please explain whether, in your opinion, this consultation was adequate, and, if so, why.

Answer: Senior managers of the FAM and Explosives Unit programs were involved in the pre-decisional discussions and development of alternatives. The senior leadership of the programs provided our link to the affected employees during the decision making process. Once decisions were made, those managers have been responsible for working

with employees to ensure a smooth transition to the Bureau of Immigration and Customs Enforcement.

28. On September 2, 2003, DHS announced the creation of a new Customs and Border Protection (CBP) Officer position, effectively merging three existing inspectional workforces – Customs Service, INS, and APHIS. What consultation did top officials of the Department undertake with affected senior managers before the decision was made, and before the announcement was made and since, to undertake this reorganization? What consultation did top officials of the Department undertake with other affected employees during those time periods? Please explain whether, in your opinion, this consultation was adequate, and, if so, why.

Answer: I am told that before the announcement of the new unified position, extensive briefings and consultations were held with senior managers within the Department. Concurrent with the announcement, officials from all three unions were notified, as were Agriculture executives and CBP Field Managers.

If confirmed as Deputy Secretary, I am committed to a consultation process to include employees and their representatives, as appropriate.

29. With the creation of the CBP Officer position, as part of the "One Face at the Border Initiative," how should the Department make sure that this unified force can essentially perform job functions that were previously done by three different specialized inspection forces?

- Should there be back-up specialty experts for various customs, immigration and naturalization, agricultural, or other disciplines? Or should every CBP Officer be expert in all aspects of both primary and secondary inspections at the border? Apparently, DHS will retain some specialized agricultural agents. Please describe.

Answer: The Homeland Security Act merged these different specialized inspection workforces to carry out the priority mission of preventing terrorists and instruments of terrorism from entering the United States while facilitating the flow of legitimate trade and travel, and to perform the traditional missions of the three legacy agencies. "One Face at the Border" establishes one-stop processing, a single officer to interact with the traveling public and trade community at the nation's ports of entry. The CBP Officer capitalizes on the skills and competencies that are common to the occupations: observation, analysis, risk-assessment, interviewing, examination, etc. Specialized Agriculture expertise must be retained to carry out duties that require undergraduate education in biological sciences.

- As newly trained CBP officers are integrated into the inspection workforce, and as the legacy Customs, INS, and APHIS inspectors retire or otherwise leave the job, what plans would you implement to combat the loss of specialized expertise in areas such as cargo examination, importation, drug interdiction, etc.?

Answer: Fortunately, CBP today has a highly trained and dedicated workforce that will be with DHS for many years to come. All new CBP Officers will be fully trained through an extensive Post Academy Training program in all aspects of the job, including cargo examination, drug interdiction, document fraud, etc. This Post Academy training will be a combination of classroom, computer-based, and on-the-job training. As these officers obtain the experience of the work, they will become the material experts in those areas. Fortunately, we have the benefit of using the incumbent officers (current material experts) as mentors and coaches for these new CBP Officers.

30. What due process rights and procedures are afforded TSA screeners who believe they have been unfairly disciplined or have otherwise subject to an inappropriate personnel decision? For example, under the applicable grievance system, do employees have the right to have an objective third-party review the matter and render an opinion? What role does the Office of the Ombudsman have in ensuring TSA screeners are afforded due process, including what authority does the Office have to obtain relief?

Answer: If a TSA screener believes that he/she has been unfairly disciplined or subjected to an inappropriate personnel decision, an employee may pursue their concerns by seeking assistance from the Office of the Ombudsman, may file a formal grievance or, if an employee believes that he/she may have been subjected to discrimination or harassment based upon race, color, religion, sex, national origin, physical or mental disability, age (40 or over), sexual orientation, or reprisal, an employee may file a complaint with the Office of Civil Rights. An employee who has completed their probationary period filing a grievance may also appeal an adverse action (suspension of more than 14 days, removal, etc.) to the Disciplinary Review Board.

If an employee is terminated due to a suitability issue he/she may seek assistance from the Office of the Ombudsman or may request a review of the facts if he/she believes the information reported in the background investigation is incorrect. A second review of the background investigation and the information submitted by the employee is conducted by the Personnel Security organization. Furthermore, after completion of the employee's probationary period, he/she may elect to submit a written response and supporting documents to the Deciding Official in response to the proposed action that outlines the negative information reported from the background investigation.

Under the grievance procedures, prior to filing a grievance, an employee may request the methods of alternative dispute resolution made available by TSA.

The TSA Office of the Ombudsman maintains neutrality in this process. They have the responsibility to consider the concerns of all parties known to be involved in a dispute, but do not take sides with any person or group. They also do not determine legal rights or make binding decisions. With this mission, they do not demand change, nor make determinations that personnel decisions might be inappropriate.

TSA is convinced that these rights and procedures available to aggrieved TSA screeners are adequate. They reflect a real commitment to reducing conflict, focusing on security and accomplishing the mission. I am also committed to a model workplace that relies on these checks and balances to increase personal satisfaction and organizational productivity.

National Strategy

31. Homeland security requires the work of the entire federal government, as well as the state, local and private sectors. The National Strategy for Homeland Security does not clearly define the accountability structure to ensure the implementation of efforts to strengthen and sustain homeland security.

What should be the appropriate interrelationship between the Homeland Security Council, he President's Homeland Security Advisor, OMB and DHS that will create the best structure for national strategy implementation and accountability?

Answer: The members of the Homeland Security Council, the President's Homeland Security Advisor, OMB and the Department of Homeland Security are united in ensuring that we are implementing the President's National Strategy for Homeland Security.

The President's National Strategy for Homeland Security outlined responsibilities and for each of the strategy's initiatives and critical mission areas and the Administration, when possible, has identified lead executive branch departments and agencies for each of the *Strategy's* initiatives. In addition, the Department of Homeland Security for the first time consolidates and focuses responsibility for critical homeland security activities – for example, border and transportation security, critical infrastructure protection, or homeland security science and technology. Furthermore, the President's Budget for Fiscal Year 2004 aligned resources of the federal government to directly support these clarified lines of responsibility and accountability. The Homeland Security Council will continue to coordinate policy among the relevant departments and agencies and provide confidential advice to the President on homeland security matters.

Funding

32. In a September 2001 article on homeland security written shortly before the attacks, you wrote that agencies with homeland security missions and non-homeland security missions will only pay necessary attention to their homeland security duties if those duties are emphasized by Congress and the Administration in appropriated budgets. Reorganizing agencies may be helpful, you wrote, but this "clear tasking, well-defined priorities and adequate resources are absolutely essential." ("Meeting the Homeland Security Challenge: A Principled Strategy for a Balanced and Practical Response," by Adm. James M. Loy and Captain Robert G. Ross, U.S. Coast Guard, September 2001).

In your view, has the Administration sent a clear message about homeland security priorities in its budget requests? Has Congress? If so, how do you see those priorities reflected in, for instance, the budget of the Coast Guard?

Answer: I do believe clear messages have been sent.

The Administration and Congress have made funding for Homeland Security a priority. Congress has appropriated $31 billion for Homeland Security for FY 2004—a funding level for Homeland Security that is $14 billion more than pre- September 11. Significant new funding above pre-September 11 levels has been provided in many areas, in particular to enhance transportation and cargo security, and to protect against biological, chemical and radiological threats. In FY 2004 alone, we will provide $4 billion to help prepare and equip our Nation's first responders and first protectors.

This is very clear to me. We did not get to our current point of vulnerability overnight. The openness of our society and the very ideals we hold dear make our security challenges enormous ones. Often in our history, a tragedy has been followed by dramatic legislation, and then taken years to sort out the fundamental program change to keep the tragedy from recurring. We are now two years from 9/11/01 and less than one year from establishing DHS. The difference with this tragedy is the combination of the states involved and the abrupt uniqueness of this new enemy compared to the Cold War. As we come to understand that enemy, I simply offer that clarity of tasking, clarity of priorities in the work and a commitment of the resources necessary to its accomplishment, are imperatives. The Administration will submit budgets with well-reasoned priorities. The Congress will react and legislate adjustments. That classic exchange will move us forward in our quest to secure America.

Such priorities are reflected in strong support for Coast Guard projects focused on Homeland Security... Integrated Deepwater System, Rescue 21, Maritime Safety and Security teams, upgraded personnel strengths and many more. Those priorities are reflected in CBP, ICE, TSA progress and many other new ways of doing business. At the end of the day, these combined efforts of both executive and legislative have brought us astonishing results to date. Our challenge is to recognize how far we have yet to go and stay the course.

Emergency Preparedness and Response Directorate

33. The Emergency Preparedness and Response Directorate is responsible for helping local communities prepare for and recover from natural disasters, and prepare for, respond to, and recover from terrorist attacks. What are the major management challenges the Department has faced in integrating specific agencies, programs, or functions transferred from other federal departments into this Directorate and coordinating its activities with other involved key federal agencies?

Answer: The integration of new personnel, programs, and functions from several agencies into the Department of Homeland Security Emergency Preparedness and

Response Directorate is certainly a significant challenge. However, it has definitely enhanced our capabilities and consolidated several key functions in one location within the department.

The Preparedness Division assumed responsibility for the Metropolitan Medical Response System (MMRS) and the Noble Training Center (Noble). Both programs were transferred from the Department of Health and Human Services (HHS) to DHS on March 1, 2003. MMRS is the only Federal program, which directly supports the local elements essential to managing a WMD mass casualty event, by coordinating hospitals, medical and mental health services, law enforcement, emergency management, public health, and first responders Fire/EMS. These linkages also enhance the jurisdictions' capabilities to manage mass casualty incidents caused by hazardous materials incidents, disease outbreaks, and natural disasters.

The Noble Training Center facilitates training for medical first responders as well as the medical community to be able to quickly identify and treat victims of a Weapons of Mass Destruction (WMD) attack. This training includes treatment modalities relating chemical, biological, radiological and nuclear assaults to ensure that all hospital personnel, including medical, engineering and administrative, are prepared to effectively treat victims. The transition challenges that DHS/EPR are actively addressing include: integration of Noble into the FEMA training system, the development and increased delivery of new curricula to the EMS and pre-hospital and hospital health community, reducing the cost of course development and delivery while increasing the number of deliveries and completing the renovation of the hospital classroom facility and the dormitories, that was begun in FY03.

The Response Division is challenged with fully integrating the National Incident Response Team (NIRT) and Domestic Emergency Support Team (DEST) assets and FEMA assets to form a more comprehensive national system that can respond to natural disasters and emergencies, including acts of terrorism. Priorities have been established for the Response Division that will address the management challenges associated with combining complex disaster response programs, creating a unified disaster workforce, and achieving new efficiencies. The consolidation and integration underway will streamline and thus help to increase the effectiveness of the management of FEMA's disaster response teams and assets.

DHS is also creating Incident Management Teams (IMT) to enable immediate deployment of more highly trained and competent leadership in any disaster environment or high threat situation. The IMTs will be an important in DHS implementation of Homeland Security Presidential Directive-5. Unlike previous emergency response teams, the IMTs will consist of standing, highly trained, and permanently rostered team members with the IMT role as their main focus and responsibility.

In addition, EPR's Response Division also inherited the Strategic National Stockpile (SNS), which has worked with the States to enhance their ability to receive and distribute SNS pharmaceuticals and medical supplies within their areas.

EPR also assumed responsibility for the National Disaster Medical System (NDMS) from HHS, which has established four National Medical Response Teams (NMRT). The NMRTs are multidisciplinary teams that include physicians, registered nurses, paramedics, emergency medical technicians, pharmacists, hazardous materials specialists, and logistics specialists. NMRTs are equipped and staffed to operate ambulatory and non-ambulatory patient decontamination lines simultaneously, as well as to establish post-decontamination patient holding areas, and their deployable team size is being expanded from 36 to 50 personnel. This change will enhance the teams' short-term patient holding capability prior to handoff to local emergency medical system authorities or an NDMS Disaster Medical Assistance Team (DMAT). Funding for NMRTs has increased more than 400 percent over the past three Fiscal Years.

Preparation and Preparedness

34. The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction concluded, in its report issued December 15, 2002, that the "threat of an attack on the Homeland is increasing." Consequently, the Panel concluded, "we must accelerate the pace of preparation to prevent, respond to, and contain an attack." Do you think the threat has increased or decreased since December 2002?

Answer: The department is certainly concerned that as time goes by, the terrorist community is trying to improve upon its ability to hurt us. DHS provides a critical component of the war on terrorism and the threats that terrorists present. The efforts to strike at terrorists and those that support them, wherever they are located, has significantly degraded, but not eliminated those threats.

35. One of the most urgent issues that we must address in order to help local communities prepare to respond to acts of terrorism is the lack of interoperability of communications systems. Currently, in many jurisdictions, local police, fire, emergency management, and other first responders are hampered by their inability to communicate across incompatible communications systems. For example, according to press reports, on September 11 New York Police Department helicopter pilots reported their assessment that the towers were likely to collapse imminently, however, they were unaware that the firefighters in the buildings could not hear their transmissions. Most recently, different jurisdictions in the Washington D.C., area had difficulties with cross-communications during the sniper attacks in October. To immediately address this issue, some have recommended that the federal government provide certain American cities with off the shelf interconnector technology that makes radio frequencies compatible through instantaneous patching systems.

- Do you agree with this recommendation? Please explain.

Answer: The lack of public safety interoperability is clearly a long-standing, complex, and costly problem for the nation. While several government programs have made great

strides in addressing this issue, much of this work has been disconnected, fragmented, and often conflicting. In an effort to coordinate the various Federal initiatives, SAFECOM was established by the Office of Management and Budget (OMB) and approved by the President's Management Council (PMC) as a high priority electronic government (E-Gov) initiative. The mission of SAFECOM, for which DHS serves as the managing partner, is to enable public safety nationwide (across local, tribal, State, and Federal organizations) to improve public safety response through more effective and efficient interoperable communications. SAFECOM has identified patching technologies such as those you describe, as a near-term, partial fix. These patches permit limited interoperability in certain situations but are not, in any way, a complete fix for interoperability.

- What other steps do you believe we should take immediately to address this issue?

Answer: The answer is not simple and there is no one-size–fits-all answer. An integrated solution will require a long-term coordinated effort among local, State and Federal stakeholders, coupled with a large capital investment and a willingness to embrace needed changes in policies. To begin to scope the framework for interoperable communications, SAFECOM has identified core focus areas in which to concentrate in order to achieve interoperability across the Nation.

1. Develop a technical foundation. The sheer size and diversity of the public safety community, coupled with the billions of dollars invested in existing communication systems, requires that SAFECOM create a framework from which to best pursue interoperability while retaining backwards compatibility with legacy systems. SAFECOM will further work to define the requirements for interoperability and develop the standards that will both guide industry as it creates solutions and guide localities and States as they purchase equipment. This will ensure that the technologies that provide the ultimate framework for interoperability are mainstream, scalable, and standards based.

2. Provide policy recommendations. Spectrum policy is an essential issue in the public safety communications arena. SAFECOM will, in concert with major State and local public safety organizations, play a key role in representing the views of local and State stakeholders on spectrum issues within the Federal government.

3. Coordinate funding assistance. To ensure that Federal money is efficiently spent and does not inadvertently create stovepiped systems at the local and State levels, SAFECOM will help the Federal government tie grant funding for public safety communications planning, equipment, training, and assistance to consensus grant guidance. In addition, information about best practices, grant funding, and equipment purchases will be made available to the public safety community through a central repository.

4. Provide technical assistance. Planning for, implementing, training on, and maintaining public safety communication systems are major tasks requiring resources many public safety agencies don't have. Hence many localities and States will need technical assistance to achieve the goal of interoperability. While there are various Federal efforts

providing assistance to local and State agencies, SAFECOM will serve as a coordinator of these initiatives as it supports the development and promulgation of coordinated best practices.

5. Coordinating Funding Assistance. In FY 2003, SAFECOM developed grant guidance in line with the needs of public safety for use by Federal programs funding public safety communications equipment to State and local agencies. COPS, FEMA, and ODP incorporated this guidance into their public safety communications grants. SAFECOM, along with the AGILE Program, assisted FEMA and COPS in coordinating their grant administration processes by supporting the development of the beta version of a database clearinghouse on communication grants. This Grants Clearinghouse will help eliminate unnecessary duplication of funding and evaluation efforts.

6. Technology Development. In FY 2003, SAFECOM completed the initial draft of a Statement of Requirements (SoR) for public safety communications. This SoR is the first comprehensive document on the functional requirements for public safety communications, and will serve as SAFECOM's basis for its technology efforts. SAFECOM is gathering input from industry on current technologies available or under development to enhance interoperability. This effort will enable SAFECOM to ascertain what technologies and products exist so that the program can more specifically focus on promoting the acceptance of such technologies through demonstration projects.

7. Technical Assistance. SAFECOM is developing an interoperability information portal that will provide information to public safety agencies through an integrated, central site. This site will serve as a one-stop shop for public safety agencies. The site will also include tools such as a "scorecard" that will be used to identify and track public safety's progress on interoperable communications. Much of this education and outreach will leverage the work of the former Public Safety Wireless Network program, which has now been absorbed by SAFECOM.

36. Currently, it is primarily the responsibility of the private sector to improve the preparedness of the nation's chemical plants and trucking system. However, given the serious consequences for our nation that could result from a successful attack on a chemical plant or a truck carrying hazardous materials, there is significant concern that the federal government must do more in this area.

- What role do you believe DHS should play in improving protections for chemical plants and trucks carrying toxic materials?

Answer: There is a DHS role, in full partnership with industry, which can reduce vulnerabilities for chemical plants and trucks carrying toxic materials. Generally, the DHS role would be within the Information Analysis and Infrastructure Protection and Science and Technology Directorates.

- Do you believe that stricter federal regulation is required for chemical plants and trucks carrying hazardous materials?

  Answer: The President has stated that we will work with Congress on legislation for chemical security. We support legislation which would not subject facilities to multiple statutory schemes to prepare vulnerability assessments and security plans but would protect vulnerability information from public disclosure and would result in a more level playing field of preparedness across the industry for terrorism attacks. We would work closely with the DOT on necessary enhancements to security in the transport of hazardous materials as well.

Science and Technology Directorate

37. As the Directorate of S&T will bear primary responsibility for developing new technologies and mapping available technologies to the needs of other Departmental entities and first responders, it is crucial that the Department coordinate its activities between the various directorates and their Under Secretaries. For example, regarding border and port security, the Directorate of Border and Transportation needs to acquire new technologies for detecting and tracking cargo that may contain nuclear, radiological, biological, or chemical agents. This need may require further assistance from the Directorate of S&T to support the development of innovative sensor and tracking technologies, or to identify and acquire commercial available technologies capable of providing the required functions.

    Do you believe that the R&D, funding, and technology acquisition efforts of the Directorate of S&T is sufficiently coordinated and aligned with the needs of the other Directorates? How can the existing system be improved?

    Answer: The purpose of DHS S&T is to ensure alignment with the National Strategy and implement an overall DHS/S&T strategy. The DHS/S&T strategy includes coordinating and incorporating the strategies of individual components such as the Directorates of Border and Transportation Security (BTS), Emergency Preparedness and Response (EPR) and Information Analysis and Infrastructure Protection (IAIP); the United States Coast Guard (USCG); and the United States Secret Service (USSS), to ensure our S&T efforts are coordinated and aligned to support the needs of the other Directorates and operational components.

    The S&T Directorate is working very closely with the other Directorates in DHS to coordinate and integrate the RDT&E portfolio of the Department. To that end, S&T Portfolio managers also serve as liaisons to one of the operational organizations (e.g., BTS, IAIP, EP&R, USCG, USSS) with many of these staff being matrixed from their home organizations. The S&T budget directly reflects requirements identified by these end-users. In addition, the S&T Directorate has assumed government oversight for the federal laboratories that transferred into the Department in FY03. The S&T Directorate

has an Office of Federal Laboratories that is responsible for ensuring that these facilities and programs are integrated into the overall RDT&E enduring capability of the Department.

38. To assist with the identification, acquisition, and deployment of technologies developed in the private sector, the Department must coordinate with extra-Departmental entities to initiate and fund appropriate R&D. This is especially important as a large amount of research and technology efforts relevant to homeland security will continue to occur outside the direct control of the Department B in other agencies and in corporate or university laboratories.

- How do you plan to promote interagency collaboration on homeland security R&D, particularly in areas that may fall outside traditional agency missions or scientific disciplines?

Answer: Under the Homeland Security Act, we are required to coordinate with DARPA, TSWG and other relevant research agencies and we have authority to run joint programs with them. More importantly, we want to exchange research results with them for our mutual benefit.

DHS S&T has an informal agreement with DoD to participate in their annual technical review processes and will extend reciprocal invitations to join in HSARPA technical reviews.

Additional interagency cooperation will accrue from research activities conducted at Federal laboratories sponsored by other agencies, in particular, DOE.

- In regard to using resources from the private sector and academic community, what steps will you undertake to identify, support, acquire, and deploy commercially available or near-mature technologies that are capable of servicing the missions of the Department or its Directorates, such as the port security mission of the Directorate of Border and Transportation Security, or the risk analysis functions of the Directorate of Information Analysis and Infrastructure Protection?

Answer: The Department has, and will continue to have, an active outreach to private industry and the academic community to identify, acquire and deploy commercially available or near-mature technologies that are capable of servicing the missions of the Department or its Directorates. This is being done through a variety of mechanisms such those described in the response to Question 31, by competitive solicitations, and by planned "technology fairs" where the Department, usually through the S&T Directorate, can identify its needs and industry and academia can respond with potential technologies to meet those needs.

- If the Department is unable to acquire appropriate technologies in the commercial or academic sector, how will you undertake partnerships with industry or academia in developing such technologies?

Answer: Supporting research can take the physical forms of 1) issuing merit-based grants to institutions and universities, 2) letting competitive contracts to businesses, or 3) using "Other transactions" (Sec. 845) authority to contract for specific research. If necessary, we can form long-term partnerships with universities or businesses, but we believe that vigorous, open competition of ideas from the research community leads to the most desirable results in the shortest time. In urgent cases, we have the ability to conduct targeted competitions to address specific vulnerabilities identified by the HSARPA Director.

Within the constraints of classification (to prevent exposure of known vulnerabilities), HSARPA will issue public solicitations that seek new ideas, concepts, and emerging technologies from commercial firms, universities, and independent laboratories. HSARPA's first such solicitation for chemical/biological sensors and systems was issued September 22, 2003. There were 518 responses from a wide variety of universities, companies, and other research institutions.

- How should the Secretary of Homeland Security utilize the National Science and Technology Council in ensuring coordination across the federal government on the development of new technologies relevant to homeland security?

Answer: Within the National Science and Technology Council, the Infrastructure Subcommittee was created to serve as an interagency forum for developing consensus and resolving issues associated with coordinating R&D agendas, policy, and programs related to developing and protecting the Nation's infrastructure. This Subcommittee is co-chaired by DHS S&T and the White House Office of Science and Technology Policy (OSTP). For purposes of this subcommittee, R&D includes basic research, applied research, technology development and engineering, and demonstrations.

39. What are the Science and Technology Directorate's plans for spending its $75 million in rapid prototyping funding?

Answer: Last spring, DHS S&T made an agreement with the Technology Support Working Group (TWSG) to perform (temporarily) part of our statutory function of rapid prototyping for the fiscal years FY03 and FY04. DHS agreed to transfer $30 million to them in each fiscal year to fund efforts selected by them under a solicitation based on DHS-identified requirements. [The solicitation title is: Combating Terrorism Technology Support Office, Technical Support Working Group (TSWG), Department of Homeland Security (DDHS), Broad Agency Announcement (BAA), DAAD 05-03-T-0024, Issued May 14, 2003, and closed June 13, 2003.]

HSARPA will use the remaining dollars for rapid prototyping projects. For example, HSARPA will continue a maritime surveillance prototype testbed with the Coast Guard in the South Florida area that was begun in late FY03. This project combines data from radar, optical, and infrared sensors to give the Coast Guard increased maritime awareness.

During this fiscal year, HSARPA will issue more solicitations to the business and academic research community in areas such as radiological and nuclear countermeasures, conventional explosives detection, threat vulnerability and threat analysis, and cybersecurity. Each of these has the potential to generate one or more rapid prototyping efforts.

Border and Transportation Security Directorate

40. The Border and Transportation Security Directorate, which includes the border inspectors from the Animal and Plant Health Inspection Service, will have significant responsibility for protecting our nation's food supply from deliberate attack. The Gilmore Commission has concluded that there is a lack of overarching appreciation for the true threat to America's agriculture, that the nation's agricultural and food industry may be vulnerable to terrorism in ways that we may not yet fully understand, and, without a broad threat assessment, it is difficult to prioritize resources to counter the terrorist threat. Similarly, the Hart-Rudman report concluded "confusion over reporting obligations, who has jurisdiction, and to what extent they can provide adequate response to a potential attack promises to seriously compromise America's ability to contain the consequences of attacks on U.S. crops and livestock." The Gilmore Commission recommends that the President direct the National Intelligence Council, in coordination with DHS, USDA, and the Department of Health and Human Services to perform a National Intelligence Estimate on the potential terrorist threat to agriculture and food.

- Do you agree with this conclusion and recommendation?

Answer: DHS agrees with the recommendation that a National Intelligence Estimate (NIE) be performed. Undertaking this effort will provide a comprehensive assessment of threats to and vulnerabilities of the nation's food supply. At this time, the National Intelligence Council has at least one study on food security in progress.

Within the National Strategy, agriculture and food are identified as two of the fourteen critical national infrastructure sectors. While the federal agencies involved in these sectors have generally coordinated, HHS, DHS and USDA are taking a closer look at the potential terrorist threat and taking appropriate steps to mitigate that threat.

- What is your understanding of our nation's current level of preparedness for a terrorist attack on our food and agricultural systems?

Answer: USDA and HHS continue to lead the efforts of the Administration for food and agriculture safety and security. While most preparedness activities in this area are based on safety, tampering and related concerns, more can be done to ensure that equal consideration is given to terrorist attacks to these systems. At this time, DHS focus is on two biological areas: foreign animal diseases and food security.

In collaboration with USDA, DHS/S&T is developing a national strategy for foreign animal diseases, initially focused on the highly contagious food-and-mouth disease, which includes the operations, research, and diagnostic programs of the Plum Island Animal Disease Center (NY).

To address key issues in the food domain, the Homeland Security Council convened an Interagency Food Working Group (IFWG), with participation from DHS, DOD, FDA, and USDA. A major initial activity was a series of consequence-based (as opposed to threat-based) vulnerability assessments of five initial important food commodities and their production systems, as a requisite first step in the implementation of a 'Food Shield' for critical commodities.

During FY 2004, DHS/S&T is conducting an end-to-end systems analysis of one of these five food security scenarios, and plans to develop an aggressive R&D program to design and deploy detection and surveillance systems (analogous to BioWatch for pathogens of human health) at critical nodes of this important food commodity and its production system.

- What benchmarks should be used to measure our success?

Answer: Our success will be measured by the completion of specific projects undertaken to improve food and agriculture preparedness for terrorist attacks. DHS will continue to work with USDA, HHS and the Food and Agriculture ISAC to establish goals and identify benchmarks to further this effort.

More specifically, the DHS/USDA collaboration for foreign animal diseases includes an aggressive strategy to deploy next-generation diagnostics, vaccines, and anti-virals for foot-and-mouth disease. This strategy includes major milestones at 1-, 3-, and 5-year intervals, which will provide metrics by which progress of this program can be judged.

In the food domain, the design and deployment of new detection systems at critical nodes of major important commodities (again with major milestones clearly articulated), and a demonstration of the sensitivity and specificity of detection for major threat pathogens, will provide metrics by which to measure progress in this domain.

41. The Homeland Security Act establishes a number of protections for the Coast Guard's non-homeland security functions. Section 888 of the Act explicitly states that the functions and assets of the Coast Guard will be maintained intact and without significant reduction as a result of the Coast Guard's transfer into the Department. As Deputy Secretary of Homeland Security, how would you work with the DoD to make sure that the intent and purpose of the Coast Guard provisions of the DHSA are carried out?

Answer: If confirmed as Deputy Secretary, I will work to ensure the Coast Guard is able to perform all of its missions as required by the Homeland Security Act. As part of this

effort, I will work closely with the CG, other Federal agencies, Departments, OMB, and the Congress.

I believe it is in the national interest to preserve a robust, seamless and interoperable relationship between the Navy and the Coast Guard. I will work with my DOD counterparts to ensure that the Coast Guard continues to remain operationally compatible with, as well as trains and operates alongside, DOD assets in support of the regional combatant commanders to ensure the Coast Guard maintains a sharp edge on its skills to perform its national defense missions. However, it will always remain DOD's decision on when and where to use the Coast Guard wartime capabilities overseas.

Regarding the specific question about working with DoD, by federal law, the Coast Guard is a military service and branch of the Armed Forces of the Unites States at all times, and the Coast Guard is required to maintain a state of readiness to function as a specialized service in the time of war. The discussion about the Coast Guard's wartime role has been, is, and will continue to be appropriately reexamined especially in a post-9/11 environment, and is part of the larger transformational military review that all services are undergoing. The Coast Guard's capabilities have never been more relevant than they are today. The service brings unique capability, authority and access with its military, law enforcement and intelligence roles. These capabilities support both the Department of Homeland Security and the Department of Defense combatant commanders. I will focus my efforts on how to efficiently and effectively provide the combatant commanders the right tools to accomplish their missions, regardless of service distinction.

FAMS and BICE

42. In your testimony on September 9, 2003, before the Senate Commerce Committee, you stated that the transfer of the Federal Air Marshal Service (FAMS) to the Bureau of Immigration and Customs Enforcement (BICE) "will create a 'surge capacity' to effectively deal with specific threats by cross-training FAMs and BICE agents to help disrupt aviation security threats." How long will it take to cross-train BICE agents, who are primarily trained as investigators, so that they can be deployed as FAMs, who are primarily trained as law enforcement officers? Will all BICE agents undergo this cross-training, or will agents be selected for this assignment? Will BICE agents be routinely deployed as FAMs or only under special circumstances? Please explain.

Answer: ICE will be able to provide additional aviation security during heightened threat environments through the tactical deployment of ICE Agents to supplement existing FAMS deployments on U.S. air carriers. Mission surge capability will also be possible as ICE Special Agents who are already traveling for work can be incorporated into the FAMS mission scheduling system to increase flight mission coverage, based on heightened levels of threat or intelligence. This concept will be developed in a phased approach, with possible deployment in January 2004, of ICE agents who have already received security air training and helped to augment the FAM force immediately after

9/11 (approximately 100). We anticipate that the specialized aviation security training of current ICE agents will begin at the 21 FAM field offices in that same time frame, and that new ICE hires will receive aviation tactical training as part of their initial training curriculum as well.

43. One of the re-organizations within the Department that has caused opposition and concern among some of those involved is the merger of Customs and INS law enforcement in the Bureau of Immigration and Customs Enforcement (BICE). Some contend that the counter terrorism mission of Customs has been undercut by the re-organization and its capabilities limited by the organizational separation of Customs investigators and Customs inspectors at airports, borders, and ports.

- Do you believe the counter terrorism mission should be a top priority for all inspectors and law enforcement officers in DHS?

Answer: The counterterrorism mission is an integral part of the Department's mission. There are many priorities within the Department, but certainly national security is the highest, if not the utmost, priority.

- What is your view of the rationale behind placing inspectors and law enforcement officials in separate bureaus within DHS (whether in legacy Customs or legacy INS)?

Answer: Working groups convened during the DHS "transition process" and they recommended several options in this regard. An important goal in creating DHS was to bring like functions together for more effective law enforcement capabilities while eliminating duplicative functions. Along those lines, it made sense to join inspections functions of the three entities: INS, Customs, and Agriculture. Likewise, it was important to join the investigative functions into one bureau. In addition to creating a more efficient law enforcement system, this also creates a force multiplier in enforcing the law. This restructuring is also consistent with the Secretary's goal of "One team, one fight".

44. One of the main reasons for creating the Department of Homeland Security was to multiply and accelerate the counter terrorist efforts of a number of different agencies. Some contend that the merger of Customs and INS enforcement has not advanced that goal. In particular, some contend that the merger has adopted more antiquated technological practices from INS rather than more advanced practices that had been in place at Customs. They believe that the shift from state-of-the-art computer systems run by Customs to outdated INS paper systems has adversely affected budget, timekeeping, travel, salary, and procurement functions.

- How would you respond to these contentions and what would you do as Deputy Secretary to evaluate the validity of these claims and make sure that modern, automated infrastructure is not lost?

Answer: An ongoing evaluation of the technological infrastructure and associated operating systems within BICE is vital to ensuring appropriate connectivity and interoperability of systems internally and within the BTS. The technological practices adopted by BICE are currently undergoing modernization as it relates to budget, timekeeping, travel, salary, and procurement processing. Modernization will eventually result in the elimination of unnecessary paper systems and they will be phased out. Additionally, BICE has deployed Liaison Officers to engage BCBP to ensure efficient resolution of issues related to both operations and infrastructure.

US VISIT

45. The US VISIT program is supposed to be fully operational at all airports and seaports by December 31, 2003. It appears as though the Department is not going to make the Congressionally mandated deadline. The Department of Homeland Security recently announced that the entry enhancements to the immigration process under US VISIT will be operative in 115 airports and 14 major seaports by early 2004. However, exit procedures will be operational in only 10 airports and one seaport. How is the US VISIT program supposed to work effectively if exit procedures are not initially available in every port where there are entry enhancements? It appears as though travelers can be checked in but not checked out. Doesn't that defeat the purpose of the US VISIT program?

Answer: The US-VISIT Program will meet the Congressionally mandated deadline to have an entry-exit system working at all airports and seaports. The Congressional mandates require that currently available information in existing databases be integrated. The US-VISIT Program already has in place the Arrival-Departure Information System or ADIS, which receives arrival and departure data for airports and seaports. It is in addition to the ADIS system that US-VISIT is implementing biometric features, designed to further enhance the security capabilities of the US-VISIT system.

These biometric features are being implemented incrementally and will be in place for entry at 115 airports and 14 major seaports on December 31, 2003. At the request of the travel industry, the biometric features of US-VISIT will not be activated until January 5, 2004, to avoid confusion during the busy holiday travel season. While the entry portion of these biometric features can be implemented at existing facilities, the exit portion of biometric security requires additional time in order to make arrangements with airports and seaports for the placement of necessary biometric workstations to record departure information. The ability to collect biometric data at exit will be implemented at a small number of airports and seaports on December 31, 2003, due to coordination with air and seaports on placement of workstations, available funding and the deliberate, phased-in approach of these new procedures.

As US-VISIT will be operational at all air and seaports by December 31, 2003, collecting the required entry and exit data through the ADIS system, we will be meeting the Congressional mandates.

46. The US VISIT program received $380 million for fiscal year 2003 and was appropriated $330 million for fiscal year 2004. In your estimation, what is going to be the final cost to fully implement US VISIT at all ports (air, sea and land) and what do you envision will be the most expensive piece of implementing US VISIT?

Answer: Large portions of the total US-VISIT solution are still under development and the Department is soliciting US-VISIT proposals along with funding profiles, expected in late January 2004. US-VISIT will be a dynamic, evolving system, which will change and adapt to meet national security needs while promoting legitimate trade and travel without compromising personal privacy. Because US-VISIT is still developing its total solution, the final cost will depend upon the solution implemented.

47. Federal law requires that US VISIT be implemented at the 50 most highly trafficked land ports of entry by December 31, 2004; and all land ports of entry by December 31, 2005. Is the Department on track to meet these deadlines and what are the biggest potential obstacles that may disrupt the schedule?

Answer: Yes, the Department is currently on track to meet these Congressional deadlines to integrate data at the 50 busiest land ports of entry, provided that adequate funding is provided to meet these goals. At this early stage, we are trying to correct the misperception of what US-VISIT does and how it may be implemented. DHS's goals for US-VISIT include enhancing our nation's security without impeding the legitimate trade and travel vital to our economic security, while ensuring personal privacy.

- As you know, the State of Maine shares over 600 miles of border with Canada and most of that is rural. What can we expect along the northern border with respect to the US VISIT program (infrastructure, process, etc.), especially at the smaller remote land ports of entry?

Answer: At this time, the US-VISIT program is awaiting proposals from private industry for the implementation of US-VISIT along the northern border. As a minimum, we will implement the same integration and data capabilities at remote land ports as we do for the 50 busiest ports. DHS does anticipate that the appropriate infrastructure, process, and solution will be put into place along our northern land border. The deadline for that requirement is December 31, 2005. Again, DHS will implement a system that enhances national security while facilitating legitimate trade and travel.

- What role, if any, will the Canadian government have in implementing US VISIT along the northern border?

Answer: At this point, the Canadian government does not have a role in implementing US-VISIT along the northern border. The Department continues to maintain a dialogue with Canadian officials on issues of common security interest, including the possibility of modifying Canadian entry capabilities so that exit data could be provided to the U.S.

48. According to a US-VISIT fact sheet released by DHS on October 28, 2003, after the exit procedures become operational in 2004, "[a]t the international departure area, visitors will see automated, self-service kiosks where they will be asked to scan their travel documents and repeat the fingerprinting process on the inkless device."

- What measures will be taken to ensure that all departing visitors use the self-service kiosks?

Answer: The self-service kiosks described in the fact sheet are being installed in a small number of airports on a trial basis by 31 December 2003. This is an alternative being evaluated for the Air Exit process. Alternative methods under consideration include capturing biometrics utilizing self- service kiosks or hand held devices at various locations at an airport facility (i.e., international gates, security checkpoints and airport departure areas) and using alternative technology to verify identity. Along with other criteria, such as cost, the alternatives will be evaluated to ensure the concerns for the degree of compliance are addressed.

In order for the kiosk solution to be effective, outreach plays a key role. Besides reaching out to the traveling public about the need to utilize the kiosks, we are offering incentives to encourage foreign travelers to use the kiosks when departing. For example, using the kiosks will facilitate a subsequent entry into the United States, and travelers are being advised that failing to use them could affect a subsequent visit to the United States. We are also putting the kiosks in highly visible areas and will have contractors there to assist the travelers and make the process as painless as possible. Finally, we are working with the airlines to publicize the exit process so the traveling public knows what to expect and is prepared upon exiting.

- What measures will be taken to ensure that visitors do not use the self-service kiosks, and then leave the airport and remain in the United States?

Answer: Again, the kiosk is one alternative we will be field testing. To prevent people from using the kiosks and then remaining in the United States, the list of people that actually departed and the list of people that used the machines will be reconciled. Those flagged as using the kiosk without departing will be referred to US Immigration & Customs Enforcement for further investigation.

49. The Travel Industry Association fears the U.S.-VISIT system may discourage tourism if there is not sufficient equipment, personnel and training to support expeditious processing and because some visitors may have privacy concerns. As Deputy Secretary, what steps will you take to ensure that U.S.-VISIT does not unduly adversely impact tourism, legitimate international student programs or foreign workers?

Answer: The US-VISIT Program and DHS have worked very hard on this issue. Studies have been conducted on how long it takes to process people, the number of

kiosks and support personnel needed. These studies have helped us to determine what will be needed to make this a smooth and efficient process.

The most important goal of US-VISIT is to expedite legitimate trade and travel without impeding the flow at the border, while serving to promote both national and economic security. DHS already has teams working with Customs and Border Protection to reengineer the inspections process. Using electronic equipment in the processing and inspection will help to speed rather than hinder the process. For example, before computers, inspectors had to look up names in a lookout book by hand, which greatly slowed things down. Now computers do the work much more quickly and effectively. We expect similar results with this program.

As US-VISIT further develops we hope to institute trusted traveler programs where low risk or pre-registered travelers can be expedited through the entry and exit processes. Finally, we need to develop a strong outreach program so people will develop confidence in US-VISIT's goals. The key to public acceptance of the US-VISIT program is an understanding of how it works, its goals and feeling reassured that the data and privacy of the citizens will be protected.

Border Crossings

50. DHS is facing many challenges in trying to improve our nation's security. Nowhere is the challenge greater than at our borders. Each year, the United States admits 330 million non-citizens through our borders. In Maine, some 4.6 million cars and trucks cross over the border from Canada each year. And the Ambassador Bridge between Detroit, Michigan and Windsor, Ontario alone carries $250 million worth of merchandise per day, which is 27 percent of the total daily trade between the U.S. and Canada. That is a lot of traffic, and a lot of opportunities for our enemies.

But there is another side to the coin. For many in Caribou, Maine, less than an hour's drive from the Canadian border, traveling back and forth between Maine and Canada to work or visit friends or family is a regular occurrence and a way of life. Family members live across the border from one another and businesses in one country depend on suppliers and customers from another in order to survive.

How do you intend to balance the imperative of securing our homeland with the need to allow the free flow of people and commerce between the United States and our neighbors?

Answer: As the question suggests, the primary mission of U.S. Customs and Border Protection (CBP) -- the Department of Homeland Security Bureau responsible for managing our borders -- is to prevent terrorists and terrorist weapons from entering the United States and at the same time to facilitate legitimate trade and travel. CBP and the Department have been achieving these twin goals, not by viewing them as mutually exclusive, but rather by viewing them as mutually reinforcing.

In other words, by building so-called "smarter borders," CBP has been able to improve both our security and the movement of goods and people. Some of the key ingredients to building smarter borders include: obtaining advance electronic information on people and goods coming to the U.S.; analyzing that data using sophisticated automated targeting systems, deploying sophisticated inspection technology to rapidly screen people and goods for terrorist threats, enhancing supply chain security by working in partnership with the private sector, and pushing our zone of security beyond our physical border. Although CBP and the Department are implementing programs on both land borders that contain all of these key ingredients, (e.g., deploying substantial amounts of Non-Intrusive Inspection (NII) technology and working with Canada to target and inspect shipments arriving in Canada that are ultimately destined for the U.S.), I would like to focus on two programs on our Northern Border that best illustrate that increasing security and facilitating legitimate trade and travel are mutually reinforcing objectives:

Securing and Facilitating Commercial Traffic

Over the last year, CBP has developed and implemented the Free and Secure Trade (FAST) program (in partnership with Canada). Under this program, shipments that are low-risk from a security perspective are given the most expedited form of commercial processing available on the Northern Border. The security against the terrorist threat in this program is substantial. Not only must the driver carrying a FAST shipment be registered with CBP, which requires a substantial background check and personal interview, but the carrier and the importer of the shipment must be participants in the Customs-Trade Partnership Against Terrorism (C-TPAT). Participants in C-TPAT commit to substantially improving the security of their supply chains against the terrorist, and the results from CBP's validation program are that these commitments are being honored. The facilitation advantages of this program are equally significant. Under FAST, shipments that used to take several minutes, if not almost an hour to clear, can now be cleared in just a few seconds. One other advantage of the FAST program should be noted: Because CBP personnel recognize FAST shipments as low-risk; they are able to focus their time and attention on other shipments that may pose significantly higher risks. Thus, the FAST program illustrates how CBP can substantially increase security and at the same time facilitate legitimate trade.

The program is currently operational at the six largest commercial ports of entry on the Northern Border and it will be expanded to seven additional ports of entry by the end of this year.

Securing and Facilitating Passenger Traffic

There is a program for frequent cross-border travelers that parallels the FAST program for commercial shipments in many respects. This program is known as NEXUS, and it has been developed and implemented in conjunction with Canada over the last two years. Under NEXUS, individuals apply to the program and are vetted by both the Canadian and U.S. Governments. This vetting process includes background checks by both

countries and a personal interview. This is a far more rigorous process than is performed via normal CBP processing at the port of entry, and thus the increase in security associated with this program is substantial. The same is true for facilitation. NEXUS participants, like FAST shipments, are offered dedicated booths (and in some cases lanes) and expedited CBP processing. And like FAST, NEXUS allows CBP to focus its inspection efforts on other passenger traffic that may pose substantially greater risks.

This program has been implemented at the 7 largest passenger crossings on the Northern Border, and there are plans to expand it to several additional crossings over the next several weeks and months.

51. Earlier this year, the Department of Homeland Security Bureau of Customs and Border Protection eliminated the Form 1 Pass and the electronically read Port Pass. Residents and landowners on Maine's western border with Canada have grown to depend on the Form 1 pass as their method to enter Canada while the border crossing was not staffed. Maine residents on Maine's Eastern border with Canada have depended on the electronically read Port Pass. Since both of these programs have been eliminated by DHS, Maine residents have had their access to medical and religious services, family events, social activities, family events and other personal errands severely limited. This situation is mirrored across the United States / Canadian border.

- DHS is now using technology to speed processing at some of this nations busiest border crossings. What would be your plans to provide technology at remote border crossings so that its more rural citizens may have their free movement returned to them?

Answer: CBP is continuing to examine alternative measures for access to the border after hours at certain remote locations for registered travelers. When we are confident that a cost effective technological solution can provide a means to adequately screen vehicles and its occupants before allowing entry into the U.S. without introducing unacceptable risks, CBP may reevaluate the use of a secure, remote inspection type of system.

- Many of the technologies for personal identification already exist and are being use by the Department of Defense and other branches of government and private industry. What do you believe the timeline would be to establish personal identification technology at our remote borders with Canada?

Answer: CBP has implemented innovative programs for registered travelers, i.e., NEXUS and FAST to facilitate the movement of people and goods into the U.S. This technology currently uses personal identification technology. While the participants in these programs are considered "known" travelers, they are still required to interact with CBP inspectors at designated open ports of entry, and are not permitted free movement across the border at remote locations after normal business hours.

- Can this technology be implemented in a way that ensures a secure border? Please explain.

Answer: The Department's approach to border security is multilayered. No one technology will provide a guarantee of security. However, the FAST, NEXUS and SENTRI driver ID card hardware and software is a proven technology. These enrollment programs are as follows:

- FAST—The Free and Secure Trade Program is utilized for commercial truck drivers entering the US;
- NEXUS—is utilized for vehicle passengers crossing the US/Canada border;
- SENTRI—the Secure Electronic Network for Travelers Rapid Inspection is utilized for vehicle passengers crossing the US/Mexico border.

The FAST, NEXUS and SENTRI driver radio frequency identification (RFID) cards are similar to a driver's license and are the size of a credit card. The card is low cost, and the embedded RFID technology requires no battery.

Individuals undergo background checks prior to receiving these cards. As they cross the border, they are regularly checked against a number of databases to ensure a continued basis for a security determination.

Port Security

52. The Transportation Security Administration is expected next month to announce the third round of port security grant recipients. What weaknesses in the program, if any, were identified in the first two rounds and what improvements has the Department made to the evaluation process to address these weaknesses? How has the selection board for these grants evaluated the needs of applicants if not all eligible entities completed the vulnerability assessments on behalf of the Coast Guard? Were ports where assessments had not been completed eligible for grant money?

Answer: TSA has administered a thorough, multi-tiered evaluation process of competitive grant applications, in partnership with the U.S. Coast Guard and the Maritime Administration (Department of Transportation), to ensure fairness and consistency. The evaluation process was published in a Program Announcement/Request for Applications inviting applications, and included a local/regional review, State level review, national level review, and executive review; with a selection board consisting of the TSA Administrator, the MARAD Administrator and Commandant of the U.S. Coast Guard making the final award selections.

TSA has introduced several improvements to the application and evaluation process based on lessons learned from previous rounds. It was evident after the initial Round of grants that applicants needed to provide more explicit information in their applications to successfully compete. A set of "Frequently Asked Questions" (FAQs) has been developed for prospective applicants, and it is updated each round. In particular, many project applications lacked sufficient detail, particularly regarding how the proposed

mitigation strategy is linked to the results of a completed security assessment. Subsequent guidance has been provided as to the attributes of a successful application.

53. After the second round of grants were awarded this past summer, we were surprised to see several private entities had been awarded disproportionately large amounts of funding. For example, the oil company CITGO in Lake Charles, LA, received a more than $13 million grant. The entire state of Maine received just under $1.3 million. How does the Department ensure that its evaluation process spreads funding appropriately across all well-justified grant requests?

- What is the Department's policy on providing port security grant funds to non-governmental entities and why?

Answer: Port security remains a shared a public/private responsibility, and the government currently awards grants to both. TSA's competitive Port Security Grant Program provides federal assistance to critical national seaports for security enhancements identified in security assessments.

The Port Security Grant Program evaluation process incorporates a multi-level, interagency review which includes: a *local/regional review* by Coast Guard (USCG) Captain of the Ports and Maritime Administration (MARAD) Regional Directors to verify applicant eligibility and rank applications based on risk/mitigation; a concurrent *State level review,* where designated State Representatives may elect to review and prioritize grant applications received from their respective states; a *national level review* which consists of technical subject matter experts from the three agencies (USCG, MARAD and TSA); and an *executive review* with agency representatives from USCG, MARAD, and TSA evaluates the proposed grant awards from an overarching national perspective. The *selection board*, which consists of the Administrator of the TSA, the Administrator of the MARAD, and the Commandant of the USCG (or their representatives), makes the final award selections.

54. Coast Guard regulations to implement the Maritime Transportation Security Act of 2002 are scheduled to take effect on November 22, 2003. The rules will apply to approximately 10,000 domestic ships and 5,000 waterfront facilities. The Coast Guard has estimated that affected maritime stakeholders will spend more than $1.5 billion in the first year alone to comply with the regulations and make the necessary security upgrades. Maritime officials have expressed concern over the costs and are seeking relief through the port security grants program. In what ways can the Department assist the industry in complying with these regulations that are designed to tighten port security throughout the nation? Do you think the port security grant program should be expanded?

Answer: As noted above, improving our nation's port security is a shared public-private responsibility. Federal, state, local government as well as the private sector entities in the port community all have a role to play. The Coast Guard, in the person of the Captain of the Port, provides federal leadership at the local level in this effort, working in close

partnership with the port authority and any number of local players. DHS presence also includes the work of Customs and Border Protection in cargo and container security. Both these agencies represent a significant federal commitment to security at our nation's ports. Furthermore, DHS support of state and local first responders assists overall preparedness, including at our nation's ports, in the event of natural disasters or terrorist acts.

By the end of this year, the federal government will have provided more than $500 million in port security grant funding to assist public and private entities in tightening port security throughout the nation. The grant program has been efficiently and expeditiously managed, awarding projects based on national security priorities and sound criteria. The Department will continue to assess our nation's vulnerabilities and assist states and localities in protecting our critical infrastructure.

- Please describe the criteria through which port security grants are awarded.

Answer:

- Recognizing that port security is a public and private shared responsibility, the Department awards grants to provide assistance in meeting national security needs.
- Maritime stakeholders are due to submit their security plans to the U.S. Coast Guard by December 31, 2003. TSA anticipates the next round of port security grant applications to reflect the security needs indicated in these plans and will be reviewed accordingly.
- Under Round 3 of Port Security Grant Program, TSA published the following evaluation criteria:
- Proposal must demonstrate why the port, multiple terminals, terminal or U.S. inspected passenger vessel or the nature of their operations (vulnerability/criticality/risk) justifies funding.
- Movement of hazardous cargoes or high number of passengers.
- Movement of high volume (tonnage) or value cargoes.
- Eligible applicants that have made prior security enhancements/investments.
- Cost-sharing for the proposed project.
- High probability of successful implementation.
- Impact of not implementing proposed solution/approach.
- The proposed approach is technically sound and clearly addresses the vulnerabilities identified in the Port, Terminal, or Vessel Security Assessment.
- The proposed cost/request for funding is realistic when compared to the proposed solution.
- Realism of the proposed schedule for project implementation.
- Realism of the proposed methodology.

55. The Coast Guard has estimated that following initial implementation of the MTSA, the annual cost to industry will be approximately $884 million. Over the next ten years, costs are expected to total $7.3 billion. Do you think grant programs are the best way to offset these costs for industry, and if so, why? If not, how could a more permanent

revenue stream be built into the system to fund port security?

Answer: First, let me assure you that complying with the requirements of the MTSA is one of DHS' highest priorities and essential to demonstrating the U.S. commitment to Port Security.

The Coast Guard's FY04 Appropriation contains nearly $100M for items specified in the MTSA such as Maritime Safety and Security Teams, Automated Identification Systems, and positive vessel control activities (previously called Sea Marshals). The Coast Guard's FY04 Appropriation also contains another $88M in new boats, cutters, and shore station infrastructure that will be used to enhance the security of the marine transportation system. This, however, does not fully fund MTSA implementation.

However, the federal government has also awarded significant funding to public and private port entities to bolster port security efforts. By the end of this year, the federal government will have provided more than $500 million in port security grant funding to assist public and private entities in tightening port security throughout the nation. These funds have been provided for critical security improvements.

56. The Coast Guard is expecting some 10,000 security plans to be submitted by vessels and facilities for review and approval beginning next year. The Commandant has estimated that the start up of this oversight program alone will require $70 million and 150 full-time personnel. To date, no funding has been appropriated for implementation of MTSA. How is the Coast Guard absorbing this extra workload without additional resources? Do you think additional funds for this purpose would be helpful?

Answer: First, let me assure you that complying with the requirements of the MTSA is one of DHS' highest priorities and essential to demonstrating the U.S. commitment to Port Security.

While the Coast Guard's FY04 Appropriation does not include funding for vessel and security plan review, not all aspects of the MTSA have been unfunded. For example, the Coast Guard's FY04 Appropriation contains nearly $100M for items specified in the MTSA such as Maritime Safety and Security Teams, Automated Identification Systems, and positive vessel control activities (previously called Sea Marshals). The Coast Guard's FY04 Appropriation also contains another $88M in new boats, cutters, and shore station infrastructure that will be used to enhance the security of the marine transportation system. This, however, does not fully fund MTSA implementation

The Coast Guard will also internally reprogram resources as necessary in FY04, but at a cost to other critical initiatives. The details of the reprogramming will be outlined in the Coast Guard Fiscal Year 2004 Final Operating Stage Financial Plan that will be provided to Congress. We are also working with the Administration to ensure appropriate resources are included in the Fy05 budget submission.

57. The Customs Trade Partnership Against Terrorism (C-TPAT) is a program designed to encourage higher standards and best practices within the container trade community. In return for participation, the Bureau of Customs and Border Protection (CBP) provides expedited processing and the assignment of a lower risk-analysis score to shipments from these companies. This program requires that CBP validate the processes of each member of the trade community who voluntarily participates. I understand that more than 4,000 companies have volunteered for C-TPAT, and CBP is working to provide an initial validation of each company. What is the Department's plan to provide follow-up audits after these initial reviews to ensure that participating companies continue to invest in security over the long term?

Answer: Upon signing a C-TPAT Memorandum of Understanding (MOU), companies must conduct a security self-assessment of their supply chains and submit to U.S. Customs and Border Protection (CBP) a security profile detailing the security within their company and the security required of their supply chain partners. Headquarters CBP officers review the security profile for detail and determine its acceptability. Members are also vetted utilizing multiple CBP and federal law enforcement databases. The vetting process researches if there is any adverse information on the company that would preclude it from belonging to the program. A successful vetting and security profile review results in the company receiving C-TPAT benefits, including reduced inspections.

C-TPAT validations are used to physically verify the elements of the security profile in a manner that is conducive to share best practices and make security recommendations, beyond what was submitted in the original security profile. Validations consist of both foreign and domestic visits and meetings. Validated companies receive their validation report and are given a specified time frame in which they must respond. Their response is expected to detail how they will address the recommendations included in their validation report. Companies undergoing and receiving positive reviews on their validation do not receive any additional benefits. However, receiving a negative review and not responding adequately may result in the suspension of benefits, and/or removal from the program.

Although validated companies receive C-TPAT benefits, this does not exempt them from targeted, regular and/or routine CBP enforcement exams, trade exams, and random exams. Using risk management principles, CBP will revisit or revalidate companies to ensure that security standards have been retained or improved upon.

Visa Program

58. DHS has deployed officers to Saudi Arabia pursuant to section 428(i) of the Homeland Security Act to monitor visa issuance in Saudi Arabia. What impact has the presence of those officers had on visa issuance in Saudi Arabia?

Answer: The Visa Security Officers (VSOs) in Riyadh and Jeddah, Saudi Arabia began oversight and review of all immigrant and non-immigrant visa applications prior to

issuance of a visa by Consular Officers on October 4, 2003. The VSOs have established a positive DHS presence and a collaborative relationship with the Consular Staff. Through the additional law enforcement reviews of the information in the applications, the VSOs have added the critical homeland security perspective and expertise to the visa issuance process.

59. The internet-based Student Exchange and Visitor Information System (SEVIS) is designed to collect, maintain and manage information on international foreign students, exchange visitors, and their dependents during their stay during the United States. Administered by the Bureau of Immigration and Customs Enforcement (ICE), SEVIS was designed to improve the process through which foreign students and exchange visitors gain admission to the U. S. We understand that foreign applicants are limited to the SEVIS list of approved schools, and that the State Department will not issue a visa for a student who enrolls in a school not on the SEVIS list. By what criteria does SEVIS evaluate schools placed on its approved list? Does the SEVIS list require an institution to be accredited by an organization recognized by the Department of Education? What protections are built into the SEVIS process to prevent foreign students from obtaining a student visa by providing proof of enrollment at a non-accredited school?

Answer: Starting in October 2002, as stipulated by law, all schools that enroll foreign students have been required to receive approval or certification by the Student and Exchange Visitor Program (SEVP). Certification verifies their knowledge of the requirements of SEVP and how to employ the Student and Exchange Visitor Information System (SEVIS). The primary regulation that determines the basis for school certification is 8 CFR 214.3 Approval of schools for enrollment of F and M nonimmigrants. It cites four general criteria for approval of schools [8 CFR 214.3 (e) (i-iv)]:

(i) It is a bona fide school;
(ii) It is an established institution of learning or other recognized place of study;
(iii) It possesses the necessary facilities, personnel, and finances to conduct instruction in recognized courses; and,
(iv) It is, in fact, engaged in instruction in those courses.

Most schools receive accreditation from academic or professional associations, or from other governmental agencies. That accreditation certifies that the four criteria (above) are met. SEVP is required to verify that an applying school has current accreditation. SEVP must keep some documentation on file related to how the school met that accreditation. However, SEVP does not verify or second-guess determinations of the accrediting source.

For those schools not accredited by an academic or professional association, or from governmental agencies, the SEVP certification process must replicate the accrediting function. Consequently, the SEVP certification of schools in this group requires more documentation and the process is more complex.

Beyond the issue of accreditation, SEVP certification must clearly establish that the applying school:

- Understands the national security need for compliance with SEVP;
- Has necessary computer hardware, is competent with the SEVIS software, and is able to interact effectively with students, other schools, and SEVP through the SEVIS database;
- Is knowledgeable of the requirements that the SEVP places on the school, as enumerated in 8 CFR 214.3; and,
- Recognizes potential consequences to the student, the school, and the nation by failing to comply with these requirements.

Regarding schools without accreditation from academic or professional associations, experience since October 2002 has demonstrated that truly bona fide schools, irrespective of their accreditation, have been able to receive certification.

SEVP is confident that all SEVIS certified schools have met the legal requirements of that recognition. However, we actively seek to improve the effectiveness of the certification process. Consequently, as of November 1, 2003, processing and adjudication of I-17 school certification applications have been centralized at the SEVP office in Washington, D.C. This movement reflects a clarification of responsibilities among elements of the former Immigration and Naturalization Service that have been relocated within two agencies of the Department of Homeland Security (DHS), i.e. the Bureau of Citizenship and Immigration Services and the Bureau of Immigration and Customs Enforcement. More importantly, this action is being taken to establish a full-time, professional work force that will be dedicated solely to accomplishing this critical process.

Consolidation will enable SEVP to better standardize the application of adjudication criteria and to institute efficiencies that will more closely serve the needs of academic institutions while protecting Homeland Security.

As of February 15, 2003, all students or exchange visitors must present a valid SEVIS I-20 or DS-2019, as applicable, to Department of State (DOS) personnel at a U.S. embassy or consulate in order to receive a visa. These documents are provided to the student or exchange visitor directly from the school or program where the student intends to enroll. Only SEVIS certified schools and exchange visitor programs can issue these forms. A number of alternate forms of identification are also required in order to confirm that the person who possesses the SEVIS document is, in fact, the person registered in SEVIS. As a backup to this procedure, DOS personnel have alternate means to affirm the SEVIS status of the individual applicant. Should circumstances indicate a need for further confirmation, DOS officials can contact SEVP headquarters, as well as the sponsoring school or program, for further clarification. Additionally, SEVIS documents include bar-coding encryption, which makes the documents resistant to unauthorized duplication.

NEXUS/FAST

60. The NEXUS Program is scheduled to be operating at thirteen sites by the Spring of 2004. One of the sites that has been surveyed and may be selected for NEXUS is in Houlton, ME. What is the status of the Houlton NEXUS site and when can we expect the NEXUS Program to be available at most U.S./Canada border crossings?

Answer: The bi-national NEXUS Coordinating Committee has been actively reviewing various sites for future NEXUS expansion, reviewing port infrastructure and the nature of border crossings to ensure that each location has a population base of frequent border crossers to support the construction of a dedicated NEXUS lane. The Coordinating Committee has completed its review of Houlton, Maine, and that location will be designated as a NEXUS expansion site. Expansion to other northern border locations is dependent upon the site being found suitable to support NEXUS and upon the availability of funding. The Coordinating Committee is currently identifying additional sites to be surveyed.

61. The Free and Secure Trade (FAST) Program was developed to create a process that will expedite the clearance of commercial shipments at the border while ensuring the safety and security of those goods. Houlton, ME has been designated as an Enrollment Center for FAST and should be operational by the end of the year. What is the schedule for expanding FAST and when can we expect FAST to be available at most U.S. Canada border crossings?

Answer: CBP has aggressively rolled out the FAST program to 11 ports on the Canadian border over the last year. We anticipate an even larger number of ports becoming FAST-capable by the end of 2004. However, the FAST roll-out schedule has not yet been approved by the Commissioners of Customs and Border Protection and the Canada Customs and Revenue Agency (CCRA). This topic is on the agenda for the next Shared Border Accord meeting in Toronto, Ontario, which is scheduled for January. Upon finalization of the proposed FAST roll-out plan, a formal announcement will be made.

Transportation Security Administration

62. Some believe that consistent security policy across all modes of transportation is necessary to counter the tendency of terrorists to simply shift to softer targets. A lot of work has been done to secure airline passenger travel, which could theoretically be duplicated in other modes of transportation. What do you think of the possibility of expanding passenger screening programs, such as CAPPS II, to bus, train, cruise ship, and ferry passengers? Is such an expansion contemplated? Is it necessary? Why or why not?

Answer: CAPPS II is still under development. It is intended that CAPPS II will identify terrorists and other high-risk individuals before they board commercial airplanes.

CAPPS II will conduct a risk assessment of each passenger using national security information and information provided by passengers during the reservation process-including name, date of birth, home address and home phone number, and provide a "risk score" to TSA. The "risk score" includes an "authentication score" provided by running passenger name record (PNR) data against commercial databases to indicate a confidence level in each passenger's identity. Should the decision be made to duplicate aviation pre-screening programs to help secure other modes, CAPPS II is obviously a platform that will be considered.

63. The recent disclosure that over a million JetBlue passengers had their personal information disclosed to a U.S. Army data-mining contractor has raised further concerns about programs like CAPPS II. Although the Department has repeatedly claimed that it will not use data collected for screening purposes to examine credit histories and similar information in commercial databases, reports are that Torch Concepts may have done precisely that in its research for the Army. Were the reported contacts between TSA and the Army contractor, Torch Concepts, related in any way to CAPPS II? Has Torch Concepts done any work for TSA related to CAPPS II?

Answer: Torch Concepts has not performed any work for TSA related to the development or operation of CAPPS II.

The extent of TSA's contacts with the Army contractor, Torch Concepts, were limited to a single briefing TSA attended in May or June of 2002, which was set up and attended by DOD. At the time, TSA understood Torch Concepts to be working on an application that would conduct a risk-evaluation of commercial airline passengers arriving in the area of a military base to determine the level of risk that was posed to the base at any given time. TSA was interested in learning more about the Torch Concepts approach because, at the time, TSA was actively considering various ideas for the ultimate concept for CAPPS II. The briefing on the Torch Concepts application gave TSA the opportunity to learn about a sister agency's potential approach to aviation-passenger risk evaluation.

At the briefing, DOD asked for TSA's assistance in obtaining the PNR data that Torch Concepts needed to provide a proof of concept for its application. TSA provided that assistance only in the form of an introduction for DOD to JetBlue Airlines, after JetBlue indicated an interest in potentially supporting DOD's efforts in this area. TSA did not facilitate, negotiate, or otherwise participate in any arrangement DOD and JetBlue ultimately reached regarding the provision of PNR data for the Torch Concepts project. TSA's limited efforts in this area were not related to CAPPS II.

64. Have any contractors working on CAPPS II used any real world data for testing purposes, such as that obtained on JetBlue passengers? If so, how and from whom was the data obtained?

Answer: No. TSA has not used any PNR data to test any of the functions of CAPPS II. TSA is using certain information provided by volunteers, many are DHS employees,

including both Admiral Loy and Nuala O'Connor Kelly, the DHS Privacy Officer. While CAPPS II testing will continue, and while TSA will ultimately use actual passenger data to conduct its tests, no security determinations will be made with regard to any passenger until a Final Privacy Act Notice has been published. Furthermore, as required by Section 519 of P.L. 108-90, during the permitted testing phase of CAPPS II, "no information gathered from passengers, foreign or domestic air carriers, or reservation systems may be used to screen aviation passengers, or delay or deny boarding to such passengers."

65. On May 6, 2003, in testimony before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, you testified that the purpose of CAPPS II was limited to identifying foreign terrorists and their associates and keeping them off airplanes. In response to questions, you emphasized that CAPPS II would not access law enforcement databases to search for criminals wanted on domestic warrants. You explained that you were "enormously concerned" about mission creep, and that "we will build such concerns into the privacy strategy that we have for CAPPS II." On August 1, 2003, the Transportation Security Administration released an interim Privacy Act Notice for CAPPS II, announcing that testing of elements of the controversial airline security program was beginning. The notice disclosed that CAPPS II would be used to identify individuals with outstanding federal or state arrest warrants for crimes of violence. The notice also disclosed that CAPPS II would be linked with the U.S. VISIT program.

- Why did TSA change its position on using CAPPS II to identify wanted criminals? Would the purpose be to apprehend criminals, or does TSA now believe there is a nexus to commercial aviation security?

  Answer: The CAPPSII mission is, has been, and always will be, to prescreen air passengers to promote aviation security. One of the reasons that the Department of Homeland Security was created was to capitalize on synergies offered by the various component agencies to efficiently and effectively secure out homeland. At issue is the source of potential threats to homeland security. As we have seen, they can come from within as well as outside our shores, and can include the threat violent fugitives can pose to the traveling public. As part of our commitment to keep the skies safe and defend the homeland, we have an absolute obligation to prevent the most violent of criminals from taking advantage of the commercial aviation system to flee from justice. Commercial air travel should not be a safe haven for an individual subject to a warrant for a violent crime. This is in keeping with the mission of CAPPS II – defending the homeland.

  We believe that persons wanted for the most violent of crimes, specifically defined in the US Criminal Code, including, for example, murder, manslaughter, rape, and kidnapping, should be intercepted to further protection of passengers and the public in general. To those ends, TSA will, if sufficient identifying information is provided, alert the appropriate law enforcement agency in question in the event a person subject to such a warrant attempts to use commercial air transportation.

- If a wanted criminal were identified by the CAPPS II system, he presumably would not be identified until presenting himself at the airline counter or security checkpoint, neither of which are typically manned by armed law enforcement personnel. How would a dangerous fugitive be detained at a security checkpoint? Does this scenario pose an increased risk to users of airports? Has TSA consulted with airport security or law enforcement officials regarding procedures for safely detaining dangerous fugitives?

  Answer: The responsibility for enforcing outstanding warrants will continue to be handled by the appropriate law enforcement organizations. TSA will, if sufficient identifying information is provided, alert the appropriate law enforcement agency in question in the event a person subject to a warrant for a violent crime attempts to use commercial air transportation.

  While it is still under development, implementation would be similar to the No Fly list procedures. The air carrier would notify the LEO when the passenger presents himself at the ticket counter. We do not handle No Fly or Watch List passengers at checkpoints today, nor would we detain dangerous fugitives at checkpoints. Our staffs are not trained to do so. LEOs are summoned to ticket counters.

- Why would CAPPS II be linked with the U.S. VISIT program? Will CAPPS II be used to identify undocumented immigrants in the absence of any evidence that they pose a risk to commercial aviation?

- Why does the August 1 Privacy Act notice exempt CAPPS II from the Act's requirement that agencies only maintain records "relevant and necessary" to accomplish their statutory purpose?

  Answer: The CAPPS II system of records will be exempted from 5 U.S.C. 552a(e)(1), which requires an agency to "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or Executive order." To operate effectively and efficiently, this system must be exempted from the requirements of (e)(1). To acquire Passenger Name Record (PNR) data from the airlines' computer reservations systems, TSA will have to accept the PNR record as a whole, including some PNR fields that contain information that TSA does not need to operate CAPPS II. At least at the initial stages of the program, limitations in technology will prevent the airlines from filtering out these unnecessary fields before sending the PNR to TSA. As such, TSA will receive and maintain some information that is not both relevant and necessary to the operation of the system.

If and when the technology improves to permit filtering of PNR data sent to TSA, the (e)(1) exemption will still be required for the operation of this system because TSA will require airlines to provide the data contained in any general "comment" field from the PNR. Airlines use different reservation systems to collect PNR data and they use those systems in varied ways. This lack of consistency and commonality in the structure and use of PNR throughout the airline industry means that passenger data that TSA requires might be in a specific PNR field in one airline's database, but in another's database this same data may only be found in the general comment field. This is also possible within an airline's own reservation system because PNR data is entered by various persons, from airline employees to travel agents, not all of whom will enter it the same way or in the same fields. To ensure that TSA obtains the data it needs to complete its risk assessment mission, it must require that the comment field be disclosed. Because this is a general field in which airline employees can enter any data they choose about the passenger, TSA cannot ensure that the data in this field will always be relevant and necessary to the operation of CAPPS II.

Additionally, CAPPS II may use more or less information from the PNR itself depending on the passenger. For example, CAPPS II will use less PNR data about Federal employees who have already undergone an extensive background investigation because they hold security clearances, and therefore they will not be subject to additional risk assessment to be performed in the CAPPS II system. Because TSA cannot identify which individuals fall into the categories of passengers where less PNR is needed before TSA collecting the PNR from the airline, it has to collect the same amount of PNR data for all passengers.

66. In your testimony on May 13, 2003 before the Senate Appropriations Subcommittee on Homeland Security you stated that TSA was "close to the first draft of a national transportation system security plan."

- What is the national transportation security plan designed to do and when will it be released?

Answer: The National Transportation System Security Plan (NTSSP) defines the roles and responsibilities of the key players in the transportation security sector, describes the guiding documents and governing principles of the NTSSP, and explains how the Sector Specific Agent (SSA) for transportation ensures awareness, prevention, protection, response and recovery from an intentional disruption of the transportation system and describes the concept of operations lead and supporting agencies will use to develop security plans for each mode. It also identifies the means in which compliance occurs and ways in which the NTSSP is evaluated over time to measure its effectiveness.

We are meeting with other modal administrators to complete the plan's draft and put it into broader clearance. We anticipate the completion of the draft phase by the end of the first or second quarter of 2004.

- GAO testified before the Senate Commerce Committee on September 9, 2003 that this security plan is a "prerequisite" to investing wisely in transportation security. Do you agree? What criteria is TSA using to decide what security needs to fund, and in what amounts, in the absence of the national strategy?

  Answer: We do agree that a national transportation security strategy is appropriate and view the NTTSP as the document to achieve that. Between now and the NTSSP's release, and in conjunction with the NTSSP, security needs should be prioritized based on the greatest risk to the national transportation system. To that end we are actively assessing criticality and vulnerability of national transportation infrastructure to assist with that prioritization.

67. GAO noted in a report released on May 23, 2003 that "while the Transportation Security Administration has begun work on an overall intermodal transportation system security plan, it has not yet developed specific plans to address the security of individual surface transportation modes [such as rail or transit] and does not have time frames established for completing such an effort."(Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed, GAO-03-435, at 3.) When will TSA release specific plans for protecting the security of individual surface transportation modes, such as mass transit and rail?

    Answer: TSA will work with the Department of Transportation and other DHS stakeholders to develop the national transportation security plans for each of the modes of transportation. The plans will be based on guidance promulgated in the NTSSP and will be annexes to the NTSSP.

68. On May 13, 2003, you stated in response to a question from Senator Murray before a Senate Appropriations subcommittee that you could not assure her that the $58 million appropriated for Operation Safe Commerce, a pilot program to improve security of shipping containers coming into the U.S., would be spent for that purpose. You indicated that the funds might be diverted to address a shortfall in the FY 2003 TSA budget. You also informed the Senate Appropriations Subcommittee that TSA planned to cover cost overruns in aviation security by transferring not only funds dedicated for Operation Safe Commerce but also $105 million earmarked for port security grants. Although you later committed to releasing the Operation Safe Commerce and port security grant money, TSA was actually seeking to reprogram funds to cover a funding shortfall that TSA estimated to be $913 million for FY 2003.

    - When did TSA determine that it faced a funding shortfall for FY 2003? What expenses contributed to this shortfall and when were those funds obligated?

    - The Administration sought no additional funding for TSA in the FY 2003 war supplemental and requested a $500 million decrease in TSA's budget for FY 2004. Was TSA's FY 2003 funding shortfall considered when DHS submitted its homeland security funding requests for the emergency war supplemental and the

FY 2004 budget? If so, how were these requests adjusted to meet TSA's expected funding needs?

- TSA continues to have significant demands for resources, including requests for funding to defray the cost of installing Explosive Detection Systems (EDS) in airport baggage handling areas and to address transportation security needs in areas outside aviation security, in addition to its ongoing aviation security responsibilities. Do you believe TSA needs more funding than has been budgeted or appropriated to meet these needs? What will you do as Deputy Secretary to ensure that TSA is fully funded?

  Answer: Funding a brand new federal operation has been a challenge. TSA has worked closely with the Department of Transportation, the Department of Homeland Security, the Office of Management and Budget and the Congress to address funding needs. As TSA began FY 2003, screening had yet to be federalized and a significant amount of infrastructure standup remained. A final appropriation was not provided by the Congress until February 20, 2003. This was 5 months into the fiscal year and nearly 3 weeks after the President's FY 2004 request. TSA sought a reprogramming of FY 2003 funding in May 2003. In response to concerns raised by both the House and the Senate, TSA resubmitted a revised reprogramming in July 2003. The Senate accepted the plan in August and by the House in September 2003, less than a month before the end of the fiscal year. We continue striving to maximize available resources against the many needs of transportation security.

69. Under ATSA, TSA is responsible for security in all modes of transportation. To date, TSA has primarily focused on aviation security in response to the terrorist attacks of September 11, 2001. What role do you envision for TSA in improving security in modes of transportation other than aviation? When do you expect TSA to be fully engaged in security issues for these other transportation modes? What challenges does TSA face in addressing security in non-aviation transportation and how will you address these challenges as Deputy Secretary?

    Answer: TSA is responsible for 1) establishing consistent national transportation security standards across all modes, 2) monitoring compliance with these standards by transportation stakeholders, 3) evaluating risk to the system across a changing array of threats, 4) sharing threat and risk information with transportation stakeholders (public and private), and 5) in the event of a transportation security incident insuring rapid restoration of service and public confidence. TSA is currently engaged in this process through rulemaking, risk modeling and exercise contingency planning. The challenge in implementing this strategy centers on the proper balance between public and private responsibility/investment in achieving an acceptable security level.

70. Many transportation assets - such as pipelines, rail and ships - are owned and controlled by the private sector.

- To what extent does the Administration intend to rely on the private sector to take the lead on security in:
  - rail transportation
  - mass transit
  - highways
  - air cargo
  - pipelines
  - ports

- What steps does the Administration expect the private sector to take to improve transportation security in each of these modes and what will be the involvement of TSA in these efforts?

- How will the DHS coordinate the efforts of private sector entities and federal, state and local agencies that share responsibility for security in areas such as seaports?

- What specific measures will DHS take to avoid the kinds of problems encountered when the private sector was responsible for passenger aviation security?

  Answer: DHS will work with transportation stakeholders (public and private) to develop consistent security standards across all transportation modes.

  Congress' approach to aviation security clearly contrasts with the other modes of transportation in achieving adequate security. The success of transportation security rests on the close partnership between DHS and transportation stakeholders. While clearly private investment in security is expected, the threat-based risk-managed approach complemented by performance based standards – which permits achievement of security standards within an owners business model – coupled with appropriate security grants mitigates the national cost born by the private stakeholders. Aggressive inspection/auditing of compliance with national transportation security standards ensures acceptable risk to the national transportation security system.

71. According to GAO, billions of tons of cargo are transported each year on both passenger aircraft and all-cargo planes. In December 2002, GAO reported that numerous vulnerabilities have been identified in the air cargo system, including vulnerabilities in the security procedures of some air carriers and freight forwarders, and the potential for tampering with cargo during land transport to airports or at cargo-handling facilities. (*Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344.)

    GAO's report identified actions such as using explosives detection devices to screen cargo that could be used in the short term to improve cargo security and recommended that TSA develop a comprehensive long-term plan for air cargo security.

- Do you agree that additional security measures are needed to ensure the safety of air cargo? If so, what?

Answer: Yes, I concur with the GAO report and TSA is currently establishing a comprehensive Air Cargo Strategic Plan that is based on a risk-managed approach. This plan details a layered, multi-phased strategy that will address existing vulnerabilities including those identified by GAO and TSA assessments. TSA's plan builds on existing capabilities and pursues emerging technologies to ensure that we have adequately considered the expanse of the air cargo security domain. Our approach includes and addresses priority actions based on risk, cost deadlines, performance, research and technology initiatives, and a coordinated stakeholder outreach effort.

- What is TSA's timetable for putting these security measures in place? What short term measures is TSA taking? Has TSA developed a comprehensive long-term plan as recommended by GAO?

Answer: The Air Cargo Strategic Plan guides the development and implementation of TSA's enhanced air cargo security system during the FY 2004 through FY 2008 time period. TSA will issue a Notice of Proposed Rulemaking as well as operational plans for implementation that will be updated on a yearly basis. It is important to emphasize that different program elements are at various stages of development. Certain programs are currently operational, while others are at the pilot stage or under development. In other areas, we are at the concept stage, establishing requirements and scope. For example, TSA has released a number of Security Directives (SD's) implementing among other measures random screening of known shipments of cargo. On the other hand, the cargo prescreening system envisioned by TSA to identify high-risk cargo will undergo initial field test in FY '05. The plan, therefore, addresses these programs to varying levels of detail and recognizes that TSA's overall vision for air cargo security will be achieved in phases.

- Are sufficient resources currently available to undertake these efforts and, if not, what will be required?

Answer: Yes, the baseline for the TSA plans is the level of funding recently appropriated by Congress for FY '04. Congress has provided TSA $85 million in '04 and TSA has identified $15 million from FY'03 to support air cargo initiatives. The current TSA staffing plan calls for the hiring of an additional 500 field inspectors - 100 per year starting in FY '04. The FY '04 budget includes $16 million allocated for the hiring of the first 100 inspectors. TSA will rely on this additional staff to ensure compliance with the cargo security regulations as well as build and foster a working relationship with air cargo industry stakeholders by conducting recurring inspections. Field inspectors, working under the direction of the Federal Security Directors (FSDs), will be the primary resource for accomplishing the inspections necessary to assure compliance. TSA plans to partner with industry to ensure

adequate inspection of air cargo and therefore has no plans to hire additional federal screeners to screen air cargo.

Additionally, just days ago, DHS issued a new warning that terrorists might seize cargo planes and use them as weapons, flying them into vulnerable U.S. targets. As reported in *The Washington Post*, TSA is responding to this threat by requiring foreign air cargo companies to submit their security plans to TSA for review, as domestic cargo companies now do. ("TSA Pushes for Security in Foreign Cargo," Washington Post, November 12, 2003, p. E-1).

- Please describe these new requirements and whether they will be sufficient to address the threat described in the new DHS advisory. If not, what additional measures should be taken?

Answer: TSA is requiring security measures intended to prevent the takeover of an all-cargo aircraft. US all-cargo aircraft weighing 12,500 pounds or more and the all-cargo aircraft operations of US and foreign passenger air carriers have been previously subject to security requirements. TSA is extending those requirements to foreign all-cargo aircraft operators on flights to, from, or flying over the United States. The new measures are comprehensive and designed to protect all-cargo aircraft in the air and on the ground.

Cargo meeting TSA criteria will be randomly selected and opened to verify the contents and detect any persons that might be concealed inside. Crewmember identity and flight assignment will be verified. All persons and their accessible property transported in the cabin of the aircraft will be screened for weapons and explosives. Service personnel will also be subject to screening. Each aircraft will be searched prior to loading. Law enforcement will be immediately notified if suspicious items, prohibited items, or unauthorized persons are discovered.

Baseline measures, including personnel identification requirements, are being implemented to ensure adequate access control to aircraft, facilities and cargo. Trained security coordinators in the air and on the ground are responsible for ensuring that these measures are carried out. Procedures for notification of threats and contingency plans round out this layered approach to security for all-cargo aircraft. TSA is also increasing its inspector workforce to improve oversight.

TSA has a comprehensive Air Cargo Strategic Plan based on our goal of securing the air cargo supply chain including cargo, conveyance, and aircraft. TSA will continue to improve air cargo security through the implementation of a multiphased solution that includes screening all cargo to determine the level of risk, inspecting items determined to be at greater risk, and developing and deploying information and technology solutions. Operational and regulatory programs will support the enhanced security measures.

72. GAO's May 23, 2003 report on rail security (GAO-03-435) noted a series of unresolved issues regarding the safety and security of transporting hazardous materials by rail. Most notably, the report cited the practice of "storage in transit," in which hazardous materials are temporarily stored in rail cars while awaiting delivery to their ultimate destination, and concluded that better measures are needed to safeguard these materials while they are being stored. In addition, the report raised questions about whether companies should be required to notify local communities about the type and quantities of materials being stored in transit and about other information regarding hazardous materials shipments passing through their communities. How does DHS plan to address rail security issues that potentially endanger local communities such as "storage in transit" of hazardous materials?

Answer: It is anticipated that as part of the National Transportation System Security Plan, the Transportation Security Administration (TSA), working in conjunction with DOT and FRA, will develop a National Rail Security Plan that includes relevant rail sections on cargo security, passenger security and infrastructure security to address the security of the entire rail transportation system. Security focus areas will include but not be limited to physical security, storage in-transit security, equipment security and security training.

DHS, in coordination with DOT, is in the process of conducting a study of rail hazmat shipments from origin to destination in North America. The study will examine a supply chain for rail hazmat shipments in a specific corridor to develop a thorough understanding of the railroad security process, storage-in-transit, community and first responder notification, risk and threats to historical monuments and major venues, cities and other issues critical to hazmat security. The information collected from this system security review will be used in the establishment of security standards and training for railroad employees.

73. GAO also recommended that DHS work with the Department of Transportation to develop a risk-based plan that would help both departments assess the adequacy of rail security measures already in place as well as identify gaps that need to be addressed. When will DHS complete a specific risk-based plan to address the security of rail transportation and what role will the Department of Transportation take in developing that plan?

Answer: DHS (BTS, TSA and IAIP) continues to work closely with DOT (RSPA and FRA) to ensure that the risk-based rail security plan is developed with input and collaboration among DHS and DOT, and affected stakeholders. The goal of this effort is to achieve greater organizational alignment of initiatives, resources, and overall security efforts among agencies with a material interest in rail security.

The rail security plan is anticipated shortly after the promulgation of the NTSSP.

74. GAO testimony on November 5, 2003, before the Senate Commerce Committee (GAO-04-232T) stated that "TSA currently has limited information on the effectiveness of its

aviation security initiatives." While TSA has conducted various kinds of testing, such as covert testing at screener checkpoints, these tests have not been conducted system-wide and are not being used to measure specific screener competencies. GAO found that TSA does not collect performance information on the effectiveness of passenger screeners and has only limited information on performance in other areas.

- Are there plans for TSA to put measures in place to determine the effectiveness of its security initiatives? Please elaborate.

Answer: Yes. Although TSA does not currently have complete measures of effectiveness, it does have significant interim performance measures of its success in passenger screening, to include prohibited items identified at secondary screenings and customer complaints. In addition, numbers of pieces of data currently collected by TSA may be reviewed in combination with one another to provide an overview into where there are performance inconsistencies. For instance, passenger throughput and numbers of prohibited items surrendered, and wait times and numbers of prohibited items confiscated in secondary screening can provide very useful effectiveness insight. In addition, TSA has conceptualized more robust measures to monitor the effectiveness of its passenger and baggage screening programs and it is working to finalize and begin collecting data around these measures. TSA intends to begin reporting out on its measures of effectiveness for the passenger and baggage programs in this fiscal year.

We cannot ignore the important role that TSA's risk program plays in understanding the effectiveness of the Agency. To protect the Nation's transportation systems, the TSA must fully understand those risks specific to the National Transportation System to expertly manage them. Threats must be analyzed and assessed using an integrated approach across transportation modes. The TSA Threat Assessment and Risk Management Program uses a risk-based decision process to focus its strategies across the different transportation modes under TSA responsibility.

Through its Risk Management program, TSA is conducting criticality and threat assessments. It is monitoring potential threats to the nation's transportation system, conducting vulnerability assessments of critical infrastructures and key assets, and it maintains a dynamic database of threat, vulnerability and risk management information.

TSA Screeners

75. In August 2003, the DHS Acting Inspector General issued a report regarding TSA's Checked Baggage Screener Training and Certification. The report found that questions given to screeners as part of their final exam had often been shown to the screeners in earlier open-book quizzes. The report found that the protocol adopted by TSA "maximized the likelihood that students would pass," but that "not a single question called upon a student to demonstrate a sufficient mastery of the class content to achieve

the purpose of the training[.]" TSA has announced a review of the program and the testing materials.

- How indicative is the training program discussed in the report of other training programs within TSA and DHS more generally?

Answer: That particular training program is not at all indicative of the other TSA training programs. The practices questioned were specific to the checked baggage screener training program used during the initial rollout and not any other screener training. In fact, the contractor that delivered the checked baggage training was different from the contractor delivering other screener training. The end-of-module quizzes in question have been eliminated from the training and all test questions have been reviewed and changed as necessary. Additionally, the multiple-choice tests were only one of three levels of evaluation. In addition to the multiple choice tests, screener candidates were evaluated on their ability to operate checked baggage screening equipment by instructors using standardized checklists. Screeners were also evaluated at the end of their 60 hour On-the-Job-Training on their ability to apply proper screening techniques on test bags which had been contaminated with a trace amount of explosives (the Three Bag Test).

- Is there any review ongoing in DHS to ensure that there are not similar shortcomings in other DHS training programs?

Answer: At present there is not an ongoing DHS review of the department's training and testing protocols, however; the Federal Law Enforcement Training Center (FLETC) which conducts the vast majority of law enforcement training in the department follows the accepted industry practices for testing and evaluating students. FLETC maintains an extensive database of questions and randomly generates questions from the database to build an exam following subject matter training.

We think this was an anomaly brought about by intense timelines and misaligned measures of contractor performance. To ensure this does not happen again our staff will engage & review FLETC to share the lessons learned and ensure all training is conducted with accurate training measures. Furthermore, the Border and Transportation Security Directorate will conduct a review of the measures of effectiveness for courses conducted at the Federal Law Enforcement Training Center (FLETC) to ensure that similar shortcomings are not prevalent in current course offerings.

- What is being done to make this training program more rigorous?

Answer: Since the initial TSA Internal Affairs and DHS Inspector General investigation reports, TSA has implemented two updates to the checked baggage basic training course. A complete revision of the checked baggage training module and associated examination questions is being finalized and prepared for introduction

in early December 2003. The technical modules that cover the specific Explosives Detection Systems (EDS) and Explosives Trace Detection (ETD) equipment variants are currently under revision and are planned for introduction by the end of December 2003. Additionally, EDS operation will become a specific certification attained after the screener gains experience. This approach better supports the use of on-screen alarm resolution protocols currently being validated and allows us to test to a higher level of knowledge than currently in use.

- Has TSA examined the passenger screening program to determine whether it has deficiencies similar to those discovered in the baggage screener program? If so, what did TSA's examination reveal?

Answer: The checked baggage training course investigated by DHS IG is not indicative of other TSA training programs. The biggest area of criticism surrounded the use of identical questions on both quizzes and final exams. A review of passenger screener training examinations indicated that quiz and final examination questions are not the same.

- Is any action being taken by TSA against the contractor or subcontractor responsible for training baggage screeners? Please explain.

Answer: TSA has not taken any action against its contractor responsible for providing training to baggage screeners, as neither the contractor nor its subcontractor violated any of the terms or conditions of their contract with TSA. The course content, review and final examination for the classroom portion of the training covered basic screening instructional materials. It should be pointed out that the training was not designed to prevent failures, as there were in fact failures. The training was designed to prepare screeners for the tasks before them.

76. In a report in September 2003, GAO found that TSA has not fully developed or deployed recurrent or supervisory training programs, and that TSA collects little information regarding screener performance in detecting threat objects. What measures are in place to evaluate screener performance, and do you believe that it is important to have such measures in place? When will recurrent and supervisory training programs be implemented? Why aren't they in place now?

Answer: I fully acknowledge the importance of performance measures to evaluate screener effectiveness. Performance measures in place include: 1) Initial proficiency evaluation following 60-hours of on-the-job training; 2) Threat Image Projection (TIP) and the deployment of a new expanded library of 2400 images, with initial performance results available by early January 2004; 3) On-going annual proficiency evaluation and screener certification to be completed by mid-March 2004; and, 4) Increased probative, threat based covert testing.

Recurrent and supervisor training programs are being developed in modular format. This approach allows us to incrementally deploy each training module as it is ready. As part

of our Short Term Screening Performance Improvement Plan, we are developing and introducing modular bomb sets and weapons kits to all airports for local training and testing use by the Federal Security Directors; delivering the second and third volumes of the planned six volume Screener Performance Excellence training series; deploying the Supervisors Technical Training program; fully implementing the Threat Image Projection (TIP) training and performance evaluation program at more than 1400 checkpoints; and completing leadership training via USDA for all screener supervisors within the next 6 months.

77. While TSA has reportedly confiscated some 8 million items at checkpoints since February 2002, the cases like the recent one involving Nathaniel Heatwole raise questions about the effectiveness of screening procedures. Do you think TSA should undertake any additional training or evaluation of screeners? If so, please describe.

Answer: From April to July TSA conducted an extensive evaluation of TSA's covert test results in a human performance technology study. I recently approved a short-term screener performance improvement plan that includes several training components. The overall plan consists of a series of immediate, 6-week, 3-month and 6-month milestones leading to full implementation by March 31, 2004. Specific training initiatives include: 1) Acceleration of leadership training for all screening supervisors; 2) Development and implementation of an advanced technical course for screening supervisors; 3) Full implementation of a recurrent training program for all screeners and screening supervisors; 4) Deployment of Modular Bomb Sets and weapons kits to all airports for local training; 5) Implementation of an on-line image interpretation training module for all screeners and screening supervisors; and 6) Full implementation of the Threat Image Projection (TIP) system. TSA's commitment is to continuous learning and to always gain insight from our covert test results to continuously raise the bar on screening performance.

- Does TSA have screening equipment or measures that would have detected the items Heatwole brought on to the planes? What, if any, additional measures would you call for in light of the vulnerabilities Heatwole exposed?

Answer: The only threat item associated with this incident was the box cutter. The currently deployed x-ray equipment would have imaged the box cutters in carry-on baggage; however, disassembly of the box cutters could have presented a difficult target for screeners to identify. As an added measure, TSA has created a set of x-ray images depicting items similar to those carried by Mr. Heatwole and distributed those images to the screener workforce for training purposes.

- Do you think TSA should undertake any additional training or evaluation of screeners? If so, please describe

Answer: From April to July TSA conducted an extensive evaluation of TSA's covert test results in a human performance technology study. I recently approved a short-term screening performance improvement plan that includes several training components. The

overall plan consists of a series of immediate, 6-week, 3-month and 6-month milestones leading to full implementation by March 31, 2004. Specific training initiatives include: 1) Acceleration of leadership training for all screening supervisors; 2) Development and implementation of an advanced technical course for screening supervisors; 3) Full implementation of a recurrent training program for all screeners and screening supervisors; 4) Deployment of Modular Bomb Sets and weapons kits to all airports for local training; 5) Implementation of an enhanced on-line image interpretation training module for all screeners and screening supervisors; and 6) Full implementation of the Threat Image Projection (TIP) system.

Additionally, TSA recently deployed the TSA Online Learning Center (TSA OLC), a web-based training tool that will enable all TSA personnel, including airport screeners to continually learn and develop, ensuring the quality and job satisfaction of TSA's workforce. When we achieve full connectivity to airports, checkpoints and training rooms this application will allow the widespread screener workforce to browse centralized catalogs of training courses and immediately access an online course or request enrollment in a live classroom course. Since the TSA OLC will also continually track the educational progress of these screeners, TSA also will use the tool to ensure that the latest threat awareness information is not only transmitted, but also received, acknowledged and implemented. The OLC will further enhance TSA workforce training through the use of cutting edge technology to enable employees to participate in live, interactive, web-based training presentations and collaborative workshops. Through this TSA Virtual Classroom, the employees will be able to interact with an instructor and other students just as if they were sitting in a classroom together ...despite being perhaps thousands of miles apart.

TSA's commitment is to ongoing learning and to always gain insight from our covert test results to continuously raise the bar on screening performance.

- The Heatwole case also raises questions about airlines' own daily inspections of airplane cabins. What is TSA doing to ensure that airlines' inspections of their cabins is effective?

Answer: CFR 49; Part 1544 – Aircraft Operator Security: Air Carriers and Commercial Operators, directs Air Carriers to conduct a security inspection of each aircraft before placing it into passenger operations if access has not been controlled in accordance with the aircraft operator security program and as otherwise required in the security program. Each Air Carrier is required to adopt and carry out a security program that meets the requirements of 1544.103, with respect to aircraft security inspections. Air Carrier Inspections, Aviation Operations, TSA, conducts regulatory and compliance inspections of Air Carrier operations to ensure they are in compliance with their security program. Principle Security Inspectors from TSA Air Carrier Inspections are currently contacting air carriers to conduct reviews of the elements of their "Daily Aircraft Security Inspection" Plan, as established within their security program. Based on these reviews, a determination will be made on whether any modifications and/or enhancements are required. I've personally met with the chief operating officers of all the major airlines

and reinforced the importance of the daily inspection citing compliance inspection to follow.

78. Since March 31, 2003, TSA has reduced its screener workforce by 6,000 positions, leaving approximately 49,600 screener personnel. While TSA may need to make some cutbacks to its workforce, and TSA has recently recruited part-time screeners at airports across the country, there are still concerns about the possible negative impact of workforce reductions on specific airports and their ability to screen passengers effectively and efficiently. With these reductions in place, how does TSA plan to ensure that airport security checkpoints are adequately staffed to prevent additional passenger delays during peak travel times?

Answer: Clearly the reduction of TSA's screener workforce has had an impact on the efficiency of screening—particularly at the major airports where we have seen a noticeable rise in wait-times associated with passenger screening. While we believe we are providing the same excellent level of security to the traveling public, the use of part-time screeners will greatly assist in our ability to staff the security checkpoints, especially during peak travel periods and during the forthcoming holiday travel periods. We review our part-time hiring process on a daily basis and believe we are assessing good numbers of screeners at the major airports to support the passenger screening requirements. Along with the flexibility part-time screeners afford in staffing up during peak times, TSA has been developing an effective software tool for scheduling. Lastly, Federal Security Directors have the authority to manage their workforce as necessary to best cover their responsibilities.

79. Earlier this year, it was discovered that many TSA screeners had not received appropriate background checks. Clearly, TSA was required to hire a large number of screeners in a short period of time, but it appears that some of the failures that led to the inadequate background checks were avoidable. Do you believe that TSA exercised adequate oversight of the contractors that were responsible for the processing of screeners' applications? If not, how should such oversight be improved in the future?

Answer: TSA has established the Credentialing Program Office, with accountability for the program. The CPO reports directly to the TSA Chief of Staff. It has appropriate visibility, and staffing. TSA relied heavily on interagency agreements and short-term contracts during initial background investigations. Now, it has developed a more comprehensive, long-term acquisition strategy for its contract requirements. A program management team in the CPO manages the contracts, with a dedicated contracting officer from the Office of Acquisition.

Intelligence

80. Many in Congress believe that the Terrorist Threat Integration Center is doing work that should be done by the Information Analysis and Infrastructure Protection directorate of DHS. The Homeland Security Act required IAIP to "access, receive, and analyze law

enforcement information, intelligence information, and other information . . . and to integrate such information in order to (A) identify and assess the nature and scope of terrorist threats to the homeland; (B) detect and identify threats of terrorism against the United States; and (C) understand such threats in light of actual and potential vulnerabilities of the homeland." Can you distinguish TTIC's mission from IAIP's mission?

Given IAIP's statutory mandate, why should not TTIC be under the supervision of the Secretary of Homeland Security, rather than the Director of Central Intelligence?

Answer: DHS/IAIP is mandated to protect the homeland by independently analyzing threat-related information with domestic security concerns. As such, DHS/IAIP, as a full member of the Intelligence Community (IC), receives intelligence information not only from its component entities, but also from other IC members, law enforcement organizations, private sector partners, and state and local government entities. DHS/IAIP has DHS analysts representing the Department in TTIC, ensuring that DHS/IAIP receives information received by TTIC that is deemed relevant to Homeland Security. DHS takes primary responsibility for analyzing and disseminating information that speaks to the domestic threat picture. DHS/IAIP is not responsible for threats to American interests overseas. TTIC is responsible for analyzing all threat-related information, including threats to American interests abroad. Also, while TTIC only disseminates information with the federal government, DHS/IAIP has a broader constituency. DHS/IAIP disseminates information to state and local and well as private entities.

81. According to an October 22 article in CQ Homeland Security, the Department of Defense's Northcom command is building an all-sources intelligence center in Colorado, the Combined Intelligence and Fusion Center, "that will link together U.S. spy agencies, federal, state and local police forces."

What involvement does DHS have with this fusion center at Northcom? How does it relate to the new Terrorist Threat Integration Center and to the mission of the Information Analysis and Infrastructure Protection directorate within DHS?

Answer: Similar with other partners in the war on terrorism, the Department of Homeland Security, specifically the Information Analysis and Infrastructure Protection Directorate, will have a relationship with Northcom as a data-provider and data-recipient. Information routinely flows to, and from, DHS's Homeland Security Operations Center to the TTIC and Northcom.

Also, presently, the DHS Homeland Security Operations Center (HSOC) has regular communications with NORTHCOM's Joint Intelligence Center on items of mutual interest. That relationship is expected to grow as the NORTHCOM fusion center comes fully online. Primarily, the HSOC DoD and DIA representatives call the NORTHCOM Representative at the JITF-CT or contact the JITF-CT Weapons Fusion Center as a vehicle for communicating with NORTHCOM, but direct communications between HSOC and NORTHCOM Intelligence Center are increasingly frequent.

Examples of interaction include:

- NORTHCOM's Intelligence Center is an important consumer of DHS information, which DHS is obligated by its founding legislation to share. The NORTHCOM Intelligence Center uses this information to tailor products for use by NORTHCOM in military operations to deter, prevent, or defeat adversaries within their area of responsibility or in appropriate instances where the military is assisting civil authorities within the United States.
- DHS coordinates with the Joint Staff, DOD, and NORTHCOM on items related to CAP locations and passes information on restricted air space violations.
- HSOC analysts notify NORTHCOM whenever DHS releases threat advisories, bulletins, or other products specifically related to the DOD or NORTHCOM mission.
- The DIA/DHS analysts review the NORTHCOM homepage on Intelink for items suitable for the Secretary's Morning Briefing and other DHS intelligence products.
- Although operations often go through the NORTHCOM representative at JITF-CT, HSOC seniors talk directly with their NORTHCOM counterparts.
- NORTHCOM has expressed and intention to man a watch desk at the HSOC—an action that will facilitate the relationship between the two entities.

82. Given your experience at TSA and with the "no-fly" list, what is your view of the Administration's announced consolidation plan for the 12 terrorist watch lists in nine government agencies? Do you believe it will work, will it be more effective than before, and how will state and local authorities gain immediate access to it?

Answer: The Terrorist Screening Center (TSC) is scheduled for initial operational capability in December 2003 and will allow for a consolidated list from which to screen individuals of concern. Phase 2 of TSC's operational capability will further facilitate state and local access to the TSC's databases. When fully operational, the TSC will efficiently and expeditiously facilitate the receipt of relevant and appropriate information to approved requestors.

Terror Financing

83. The Department of Homeland Security has an important role in investigating financial crimes. However, since early this year, terrorism financing investigations have been handled primarily by the Federal Bureau of Investigation. How is the financial crimes expertise of Customs agents being put to use in investigations of terrorism financing? Do any improvements need to be made in the coordination of financial crimes investigations between the Bureau of Immigration and Customs Enforcement and the Federal Bureau of Investigation?

Answer: The Bureau of Immigration and Customs Enforcement (ICE) continues to investigate all aspects of financial crime investigations, including those that have a nexus

to terrorist financing. In addition, the U.S. Secret Service, which has been investigating financial crimes since 1865, has taken aggressive steps to partner with those in the financial services industry and utilize prevention-based measures and training to protect our financial infrastructure. However, the overwhelming majority of both ICE and Secret Service financial crime investigations do not have a link to terrorism or terrorist financing.

ICE continues to investigate such cases aggressively, and is coordinating its efforts through Operation Cornerstone, described in more detail below. ICE cases that may have a nexus to terrorism are vetted with the Federal Bureau of Investigation (FBI) in accordance with procedures established in the May 13, 2003 Memorandum of Agreement between the Department of Justice and DHS. DHS will continue to be the money laundering lead in all appropriate investigations consistent with ICE's law enforcement investigative authorities.

The Department is also enthusiastic about the Secret Service's pioneering approach to financial crimes investigations. The USSS Electronic Crime Task Force Initiative (ECTF) has established 13 task forces in cities and regions across the country. These task forces represent the cutting edge of efforts to partner with federal, state and local police departments, prosecutors at all levels, private industry and academia to safeguard our financial and critical infrastructures, and protect American consumers and industry alike. Their training and investigative techniques are innovative and unprecedented. While the MOA with the Justice Department does not include Secret Service investigations, it is the operating practice of the agency to share case information with DOJ-led Joint Terrorism Task Forces once a terrorist nexus has been established.

On July 8, Secretary Ridge announced the creation of Operation Cornerstone, a new financial crimes investigation initiative for ICE. Operation Cornerstone employs the full range of money laundering and financial crime investigative authorities that was available to the former U.S. Customs Service and which now resides in ICE.

The combination of former Customs and Immigration law enforcement authorities and jurisdictions within ICE has created an investigative bureau with unique tools to investigate money laundering offenses. In order to fully utilize the authorities of the combined agencies, the ICE Financial Investigations Division was reorganized into several sections, with Cornerstone being the central piece of the program. Cornerstone seeks to employ a methodology of identifying and attacking vulnerabilities in financial systems, and disseminating these findings to the financial and trade sectors.

Cornerstone will continue to investigate criminal violations regarding the international transportation of financial instruments, including those involving unlicensed money transmitters, the smuggling of bulk currency, and transactions structured to evade federal currency reporting requirements. ICE will also continue to investigate money laundering offenses under ICE's jurisdiction, including the laundering of proceeds derived from drug smuggling, trade fraud, export of weapons systems and technology, alien smuggling, human trafficking, and immigration document fraud.

MANPADs

84. There has been great concern about the threat posed to commercial aircraft by man-portable air defense systems (MANPADs). The threat was made clear by unsuccessful MANPAD attacks or attempted attacks in the last year in Kenya and Saudi Arabia. The Department of Homeland Security is currently assessing the technology available to address this threat, but it appears that DHS is several years from making a decision on any widespread deployment of anti-missile technology on commercial aircraft.

- What is your best estimate of when DHS will be ready to make a decision on whether to deploy such technology on commercial aircraft, and when such technology would actually be deployed?

Answer: Within two years, DHS expects that the majority of risks associated with modifying and integrating existing counter-measure equipment for commercial will be sufficiently reduced to make a recommendation for or against a low-rate production and integration program. At the end of this twenty-four month program, we will be in a position to assess potential deployment options, and initiate production as appropriate.

- What is most effective way to protect commercial aircraft from MANPADs threats in the interim period?

Answer: The Administration has employed a three-pronged strategy to countering the MANPADs threat: nonproliferation efforts, tactical countermeasures and technical countermeasures. The Department of State has spearheaded efforts to reduce the number of MANPADs on the black and gray market, making significant progress in targeting particularly concerning countries.

With respect to tactical measures, TSA, with support from the FBI, USSS, USCG and other law enforcement agencies, has completed MANPADs assessments on nearly 70 major U.S. airports, with the remaining to be completed by the end of the year. TSA also developed a self-assessment kit that has been rolled out to cover the rest of the nation's over 400 commercial airports. The results of these assessments have been shared with the appropriate state/local law enforcement and airport officials. The airport community, led by the Federal Security Director, has instituted measures to mitigate the vulnerabilities identified in the assessment process. TSA has also undertaken assessments at a number of foreign airports with service by U.S. carriers.

FAA and TSA have been working together in outreach to the air carriers, who are now moving forward on including MANPADs orientation into their pilot training courses. Customs and Border Protection is aware of the threat of MANPADs being smuggled into the nation. CBP has trained its inspectors and adjusted its targeting system to be on the lookout. As noted above, DHS has stepped out aggressively with

a program for identifying, assessing the viability of and developing MANPADs technical countermeasures in the commercial aviation environment.

This is a complex problem for which a silver bullet solution cannot be found, but the Administration is actively engaged in mitigating our nation's vulnerabilities.

Department of Defense

85. The U.S. Northern Command (NORCOM) is responsible for land, aerospace, and sea defenses. NORCOM will also help DoD deal with natural disasters, attacks on U.S. soil, or other civil difficulties, and provide a more coordinated military support to civil authorities such as the Federal Bureau of Investigation (FBI), the Federal Emergency Management Agency (FEMA), and state and local governments. How does DHS coordinate its efforts with those of DoD, particularly NORCOM?

Answer: The primary mission of the Department of Homeland Security is to protect the American homeland from terrorism. The mission of the Department of Defense is to fight and win our nation's wars. However, both the active and reserve components of the armed forces have important homeland security missions, as demonstrated by the military's activities following the September 11 attacks. Military support to civil authorities is and will continue to be a key component of the federal government's emergency response plans. Indeed, this relationship is recognized in several Presidential Directives.

It is my understanding that Office of the Secretary is currently involved in almost daily discussions with the Office of the Assistant Secretary of Defense for Homeland Defense and the Washington field office for NORTHCOM on a wide range of issues to facilitate greater interaction and coordination of collective homeland security efforts. For example, DHS and DoD are in the final stages of developing an MOA, which outlines in considerable detail the level of support that DoD will provide to DHS in terms of personnel assigned to DHS Headquarters and field offices across all directorates. The MOA also addresses the development of liaison activities between the two departments to promote greater coordination and cooperation.

Further, in August of 2003 DHS recently participated in a major NORTHCOM exercise called Determine Promise '03. This exercise occurred over a two-week period and served to strengthen operational and policy alignment between the two departments related to counterterrorism. The exercise also served to identify gaps in coordination. Should I be confirmed by the Senate, I look forward to continuing to strengthen the relationship between the Department of Homeland Security and the Department of Defense.

86. The Gilmore Commission recommended that, given the unprecedented challenges created by the Sept 11 attacks and the war on terrorism, the nation should re-examine the role of the military in responding to domestic threats. However, it said that any use of the military domestically must be carefully planned and controlled, and should be clearly

relegated to the support of civilian authorities. The Department of Defense is working on extensive R&D relevant to homeland security and has a major role to play in first responder training and capabilities through the National Guard, and in other areas. Moreover, DOD, without question, undertakes activities that protect our homeland from attack. But these are primarily military activities, which will continue to be undertaken separately from DHS. Indeed section 876 of the Act forbids DHS from engaging in military activities. And the Posse Comitatus Act, reaffirmed by section 886 of the Act, prohibits the use of the Armed Forces as a posse comitatus to execute the laws except in certain exceptional cases.

- Given the Posse Comitatus Act, what roles do you believe the military can and should play in helping civilian agencies and state and local governments prepare for and respond to terrorism?

  Answer: Congress reaffirmed in Section 886 of the Homeland Security Act that the Posse Comitatus Act has served the Nation well in limiting the use of the Armed Forces to enforce the laws and that nothing in the Homeland Security Act should be construed to alter is applicability. I do not support altering that section of the Act.

  However, the legislation also reaffirms the idea that by its express terms, the Posse Comitatus Act is not a complete barrier to the use of the Armed Forces for a range of domestic purposes. This includes law enforcement functions, when the use of the Armed Forces is authorized by Act of Congress or the President determines that the use of the Armed Forces is required to fulfill the President's obligations under the Constitution to respond promptly in time of war, insurrection, or other serious emergency.

- How will your experience in the armed forces help DHS forge the appropriate relationships with DoD?

Answer: As you know, the U.S. Coast Guard holds the unique position of being both a branch of the armed services and a domestic law enforcement agency. As such, the U.S. Coast Guard provides a perfect model to use to build a bridge between the two departments. If confirmed, I will certainly bring my experience in the armed forces to continue building an appropriate relationship between the two departments.

- Do you see any overlap in the homeland security responsibilities of DoD and DHS? Please explain.

Answer: As I stated in a previous answer, the primary mission of the Department of Homeland Security is to protect the American homeland from terrorism. The mission of the Department of Defense is to fight and win our nation's wars. However, both the active and reserve components of the armed forces have important homeland security missions, as demonstrated by the military's activities following the September 11 attacks. Military support to civil authorities is and will continue to be a key component of the

federal government's emergency response plans. Responsible and appropriate use of all federal government assets will increase our preparedness and response capabilities.

87. Defense Secretary Donald Rumsfeld has received significant attention recently for a memorandum he wrote to senior members of the Department of Defense inquiring about the Defense Department's prosecution of the Global War on Terror. Please address, from your perspective, the questions Secretary Rumsfeld poses.

- Are we winning or losing the Global War on Terror?
- DoD has been organized, trained and equipped to fight big armies, navies and air forces. Does DoD need to think through new ways to organize, train, equip and focus to deal with the global war on terror? Or, do we need a new organization? Is it possible to change DoD fast enough to successfully fight the global war on terror or is an alternative required which might be to fashion a new institution, either within DoD or elsewhere - one that seamlessly focuses the capabilities of several departments and agencies on this key problem?
- Today, we lack metrics to know if we are winning or losing the global war on terror. Are we capturing, killing or deterring and dissuading more terrorists every day than terrorist organizations are recruiting, training and deploying against us? What should the metrics be to measure progress on the Global War on Terror?
- The US is putting relatively little effort into a long-range plan to combat terrorism, but we are putting a great deal of effort into trying to stop terrorists. The cost-benefit ratio is against us. Our cost is billions against the terrorists' costs of millions. Does the US need to fashion a broad, integrated plan to stop the next generation of terrorists?
- What else should we be considering?

Answer: First, it's enormously valuable to take the time to ask such questions and I applaud Secretary Rumsfeld for doing so. We can often find ourselves fighting the tyranny of the in-basket and lose the perspective necessary to make progress both strategically and tactically. DOD's mission is to fight and win our nation's wars. That is NOT a static premise. The responsibilities of military service chiefs are to organize, train and equip their forces to fight and win. The responsibilities of theatre commanders are to fight and win. Neither of those are static responsibilities. There are two very important challenges here to be taken on. First, to recognize all the investment made by the West, led by the United States, to win the Cold War resulted by 1989 in a set of plans, protocols, tools, weapons, intelligence capabilities, etc., that got that job done. ALL of it has to be reconsidered and rebuilt to deal with a very new and different enemy. Second, the notion that served us as a nation for so many years, to fight our wars "over there", is no longer sound. So our collective challenge is one of learning all that's possible about this new enemy, transforming our tool set to become appropriate to the new threat and recognize that includes this enormous new responsibility to secure the Homeland. That requires a new vision, new strategy, new tactics, and a new tool set across the board. We

must build that capability with three basic questions to be asked. Where are we now? Where do we want to be...when? How will we know when we get there?

To those ends, metrics, compliance activities and accountability for progress along the line of accomplishment are mandatory. I look forward to working with DHS, the Administration and the Congress to identity those metrics that will recognize the threat based-risk managed approach we must use. Those choices are crucial and must represent both the long-term strategic vision as well as the tactical battles of the day. Good stewardship of the taxpayer's investment is a parallel responsibility.

State and Local Governments

88. State and local government organizations have raised serious concerns about the level of federal collaboration in certain areas, and with certain obstacles, such as access to critical data. A single contact point has been needed for state and local governments to obtain direction and assistance in meeting their preparedness needs. The HSA required establishment of the Office for State and Local Government Coordination to coordinate DHS activities relating to state and local government. This office is also to develop a process for receiving meaningful input from state and local governments to assist the development of the national strategy for combating terrorism and other homeland security activities.

- What priorities has DHS set for this office to address coordination and collaboration concerns?

- How has it been integrated with other DHS activities?

Answer: The primary objective of the Office of State and Local Government Coordination is to serve as a single contact point for states, tribes, and local governments for information about training, equipment, planning, exercises and other critical homeland security needs. The Department recognizes the importance of collaboration among federal agencies and coordination with our partners in state, tribal and local governments. To address coordination and collaboration priorities, the OSLGC is responsible for the following:

- Coordinating with the directorates and management offices of DHS to 1) better understand their relationship with state and local government, 2) determine how the OSLGC can add value to their mission and 3) facilitate DHS-wide activities to ensure coordination of activities that involve state and local governments.
- Providing guidance to the directorates in order to map current relationships and programs and to develop a process for department-wide coordination.
- Establishing strong relationships and coordinating with non-DHS departments and agencies that have a role in homeland security and are supporting state and local officials.

- Building relationships with and supporting homeland security-related activities of all state, local, and tribal governments and associations.
- Supporting states, territories, tribes and local governments through the Homeland Security Operations Center.

The OSLGC fulfills its responsibilities to state and local governments through daily interaction with state Homeland Security Advisors, local officials, emergency managers, law enforcement officials and other first responders. In addition, OSLGC coordinates with the directorates and management offices within the Department to coordinate outreach to state and local officials and implement the Secretary's policies regarding state and local government interaction. As a single point of contact for our state and local partners, the OSLGC serves as a liaison for these officials to the directorates, ombudsmen and components of DHS.

The Office's presence in the Homeland Security Operations Center (HSOC) directly links DHS with our state and local homeland security officials as well as fostering connectivity and collaboration with other federal agencies on a daily basis. The OSLGC provides a direct link for state and local officials and responders to notify the Department of incidents and share information and intelligence from federal agencies with state and local partners. Through the state and local desk at the HSOC, the Department has a direct link to communicate with state and local governments to gain intelligence about local or regional incidents of importance to the Department. In this capacity OSLGC coordinates with IAIP on a daily basis to provide critical data to assist with threat analysis and intelligence reporting.

Recently the OSLGC led the Department's development and implementation of the DHS Grants and Training Web Portal. The OSLGC collaborated with DHS components as well as other federal departments and agencies to provide a comprehensive one-stop web page for state and local officials to access information about all homeland security related grants and training offered by the Federal Government. Furthermore, OSLGC coordinates with ODP to announce new grant opportunities to state and local governments. OSLGC also manages inquiries and comments about grant programs and actively seeks feedback on ways to make to grant process more efficient and easier to use.

- What is the budget and staffing level for this office? Do you believe these levels are adequate?

Answer: The FY 2004 staffing level for the immediate Office of State & Local Affairs is 23 FTE. Its operating budget is about $3M, which is adequate for this function for this year.

89. GAO has identified at least 16 federal grants that can be used by first responders, states, local governments, and fire and law enforcement officials, to buy equipment, train, run exercises, and conduct preparedness planning. (GAO testimony: GAO-03-718T). GAO testified in April 2003 that multiple fragmented grant programs can create a confusing

and administratively burdensome process for state and local officials seeking to use federal resources for pressing homeland security needs. Problems arise, particularly, because, while different grant funds are designed to be used for the same purposes, the types of recipients, allocation methods, and grant requirements differ, thus making it difficult for state and local agencies to be flexible in their use of federal resources.

The Department has acknowledged several times before this Committee that they are aware of the concerns raised by the General Accounting Office, but has not provided any specific feedback on how it plans to address these concerns. How is the Department currently working to reduce the paperwork burden on state and local governments by simplify and streamline planning, application, reporting, and administrative requirements?

Answer: The Department of Homeland Security is committed to providing resources and assistance to states and localities in the most efficient and effective manner possible. The Department recognizes that in order for state and local jurisdictions and first responders to be effective partners with the federal government in securing our homeland, they need quick and easy access to the terrorism and emergency preparedness grant programs designed to support their work.

DHS is convinced that these programs must be more centralized and more accessible. It is our goal to provide state and local authorities a single point of contact for terrorism and emergency preparedness efforts – one access point to obtain critical grant funding. The Department's recent announcement of a "one-stop-shop" application for three different programs administered by the Office for Domestic Preparedness is an important step in this direction. The single application allows states to apply online for their allocated grants that benefit first responders and will provide additional resources to state and local government counterterrorism efforts.

This consolidation was done to streamline the grant application process and better coordinate federal, State and local grant funding distribution and operations. The homeland security assessments and strategies currently being finalized by the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, U.S. territories, and selected urban areas for submission to DHS-ODP will play a pivotal role in the identification, prioritization, and allocation of financial resources provided through the three grant programs. The funding provided will be applied against critical resource gaps identified through the assessments and prioritized in the State strategies.

Providing funds through a single application and award process facilitates coordination of preparedness activities related to the goals and objectives identified in the State strategies, resulting in a more effective and efficient use of funding. A single application also minimizes time spent on the application process and consolidates reporting requirements.

In addition to the single application, DHS is launching an interagency grants and training website on the DHS website at www.dhs.gov/grants. The website provides information

on homeland security and public safety grant opportunities offered by the Department of Homeland Security and other federal Departments and Agencies including HHS, DOJ and the EPA and a link to the Compendium of Federal Terrorism Training for State and Local Audiences, an interagency site for training opportunities available to state and local emergency personnel.

90. Other than informally consulting with other departments or agencies, what specific steps would you take to establish consistency across federal grant programs, especially those programs administered by different agencies/offices, to make it easier for states, communities, and first responders to apply for homeland security grants?

Answer: As previously stated, the Department is working to consolidate and coordinate its grant programs to facilitate a more efficient and effective application and award process for state and local agencies. As part of this effort, the Department's Office for Domestic Preparedness (ODP) recently issued a "one-stop shop" application for three separate but complementary grant programs. Under the application kit for the Fiscal Year 2004 Homeland Security Grant Program (HSGP), the Department and ODP integrated the State Homeland Security Grant Program, the Law Enforcement Terrorism Prevention Program, and the Citizen Corps Program into a single application. This joint application will streamline application process and expedite the award of funds to states and subsequently to local emergency responders.

Another example of the Department's efforts is the establishment of the Homeland Security Grants and Training Website, which provides information on homeland security and public safety grant opportunities offered by agencies across the Federal government. The Website (www.dhs.gov/grants) is intended to simplify access to these grants by placing information in a single, easily accessible site. It includes grants offered by the Department of Homeland Security as well as other Federal Departments and Agencies. Critical state and local missions supported through these grants include the preparedness of first responders and citizens, public health, infrastructure security, and other public safety activities. While these programs vary considerably in their size and scope, they all contribute to making our nation more secure against the threat of terrorism, as well as other natural and man-made hazards.

91. Senator Collins, Senator Pryor, and others have introduced S.1612, the Homeland Security Technology Improvement Act. This legislation would authorize $50 million for the Director of the Office for Domestic Preparedness to provide advanced counter-terrorism technology, equipment, and information to law enforcement agencies to help them prevent, detect, and apprehend terrorists. Do you support this legislation as reported out of this Committee?

Answer: The Department is currently reviewing S. 1612, the Homeland Security Technology Improvement Act. While the Department supports the objectives of the bill, it has several objections to the bill. First, S. 1612 is duplicative given that it authorizes

activities already authorized under the Homeland Security Act of 2002 (HSA). Under HSA, the Secretary is already granted authority to assist in the development of anti-terrorism technology, acting through various elements within the Department (see e.g. sections 302(a)-(b), 313(b)(1)-(4) (responsibilities of the Under Secretary for S&T), subtitle G (Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002)). The bill is further duplicative by establishing a technology assistance program within the Office for Domestic Preparedness. This would also result in unnecessary confusion among first responder and law enforcement communities. The bill is also narrow in scope as it addresses a technology transfer program to assist only law enforcement functions. As such, it does not address the technology interests of other homeland security missions of the Department, such as assistance to the fire service, EMS, Public health, or emergency management communities. Further, the bill vests program authority in the Director of ODP, a DHS official other than the Secretary, which is contrary to the Department's position that authorities should be vested in the Secretary.

92. Secretary Ridge and others have talked repeatedly about the Department's intention to establish a one-stop-shop for homeland security funding and other assistance. What specific steps have the Department taken or should it take -- to establish "one-stop-shopping" for state and local authorities seeking homeland security grant funding?

Answer: The Office of State and Local Government Coordination (OSLGC) within DHS serves as a first and one-stop-shop for state, tribal and local first responders for contacting the Department and specifically assists with grant funding issues. Since the Department's creation, the Secretary has been committed to ensuring an efficient and effective mechanism for distributing funds to our state and local partners. To fulfill this commitment, this month the Secretary announced the creation of a one-stop-shop webpage for Homeland Security Grant funding. This single web portal provides information on all Homeland Security granting funding both within DHS and throughout the Federal Government. This web portal also provides for the electronic filing of DHS grant applications.

In addition, the Department's one-stop-grant webpage also provides information on Homeland Security training opportunities for first responders. Accordingly, first responders now have a single web portal at which they can review and receive information about grant and training programs and opportunities.

Moreover, working with Congress, the Department was able to consolidate a number of grant programs within the Office of Domestic Preparedness. In announcing the FY 04 grants for first responders, the Department created a single web application and grant guidance document. Now, for the first time, formerly separate grant programs that once required separate applications can now be accessed through a single grant application.

93. The fiscal year 2004 Homeland Security Appropriations bill moves the administration of the FIRE Act to the Office for Domestic Preparedness. How will this affect a) the peer-review process of considering grant applications as well as other existing aspects of how the program is administered; b) whether grants would continue to go directly to fire

departments and whether any additional authorization from state or local officials would be required. Does the Administration plan on making any changes to this program beyond fiscal year 2004?

Answer: The Office for Domestic Preparedness (ODP) is working closely with the United States Fire Administration and the Federal Emergency Management Agency to ensure a smooth and seamless transition of the Fire Act Program. It is our expectation that emergency responder agencies will not be impacted in any way by the transition of the Fire Act Program to ODP. To ensure a seamless transition, ODP has met several times with USFA and FEMA officials to discuss the movement of the program. Additionally, ODP participated in the annual stakeholders meeting, which provides guidance from the field on the priorities of the program. ODP, along with USFA and FEMA officials, are working to finalize the Fiscal Year 2004 application kit and program guidelines, which should be available by early 2004.

94. During the confirmation process for Suzanne Mencer to be the head of the Director of the Office for Domestic Preparedness, the Committee asked as of July 1, 2003, how much state homeland security grant funding remained unexpended by ODP or states.

Ms. Mencer responded by saying that according to the Office for Domestic Preparedness (ODP), as of July 1, 2003, there were no unspent homeland security grant funds. But, this response only answers the narrow question of whether funding was made available to States by ODP. The Committee is concerned that red tape and other restrictions are currently hindering State and local governments and first responders' ability to access this funding once it is made available. As of October 1, 2003, what amount of ODP funds remains unspent by state and local governments?

- What steps would you take to help State and local governments access this funding in a more efficient manner?

Answer: The Department strongly supports the direction Congress provided in the FY 2003 Omnibus and Emergency Supplemental Appropriations Acts and the subsequent FY 04 Appropriations Act. It requires the Department to make funding available in 30 days, for states to apply for funds within the following 30 days, and for states to obligate funds within 60 days of the receipt of funds. These provisions provide a significant increase in our ability to ensure that funds are in the hands of states and localities in a timely manner. While we support the timely transfer of funds from the Department to the states, our ability to ensure that these funds are provided by the states and localities in a timely manner to actual emergency responder agencies is limited. Given variations in state and local law, including those related to budgeting and acquisition processes, the Department and ODP are unable to compel spending by certain dates.

95. The fiscal year 2004 Homeland Security Appropriations Bill provides $500 million for a new Law Enforcement Terrorism Prevention Grant Program. How does the Department intend to administer this program and how will the funds be distributed?

Answer: The FY 2004 LETPP seeks to provide law enforcement communities with enhanced capabilities for detecting, deterring, disrupting, and preventing acts of terrorism. The FY 2004 LETPP will provide law enforcement communities with funds for the following activities: 1) information sharing to preempt terrorist attacks; 2) target hardening to reduce vulnerability of selected high value targets; 3) threat recognition to recognize the potential or development of a threat; 4) intervention activities to interdict terrorists before they can execute a threat; 5) interoperable communications; and 6) management and administration.

The State Administrative Agency (SAA) must coordinate the implementation of this program with the State's Lead Law Enforcement Agency (LLEA). Additionally, the Department requires each State to obligate not less than 80 percent of LETPP funds to local units of government within 60 days after the grant award. If requested in writing by a local unit of government, the State is allowed to retain some or all of the local unit of government's allocation of grant funds for purchases made by the State on behalf of the local unit of government. States holding grant funds on behalf of local units of government must enter into a memorandum of understanding with the local unit of government specifying the amount of funds to be retained by the State for purchases. This agreement must be kept on file with the SAA.

In order to receive funds under this program, states must have a completed an ODP-approved state homeland security strategy. This strategy is the basis for the allocation of funds to meet prioritized needs to enhance and refine the state's preparedness efforts. There must be a clear correlation between the goals and objectives identified in the SHSS and in the FY2004 LETPP program activities.

96. The fiscal year 2004 Homeland Security Appropriation Bill provides $60 million for Competitive Training grants. How does the Department plan on structuring this program and when will this funding be available?

Answer: As you know, the states are required to update their statewide homeland security strategies and provide these to ODP by December 31, 2003. Upon receipt of the state's plans, the Department's Office for Domestic Preparedness will conduct a comprehensive analysis to identify potential gaps in our training programs. Based upon this analysis, ODP will determine training needs and issue competitive solicitations to fill those needs. It is our anticipation that the analysis will be completed in early 2004 and that a solicitation will be issued shortly after its completion. The solicitation process will be competitive, but will depend on those areas of need identified by the analysis. Once the solicitation period closes, ODP will use subject matter experts to conduct a peer-review process of the applications received and make funding decisions based on those reviews. At this point, it is difficult to give the Committee an exact timeframe for the award of these competitive grants, but the Department anticipates making final awards in mid-2004. It is our goal that the training programs that receive funding through this

program will complement existing ODP-administered training courses, thereby increasing the Department's capacity to train our nation's emergency responders.

97. In testimony before the Committee during the May 1, 2003 hearing, Secretary Ridge supported a formula that provides a base level of funding to each State. In response to a question posed by the Chairman, Secretary Ridge stated, "... I do start with the notion that every State needs a minimum level of funding ..." Do you agree that each state should receive a minimum level of funding?

Answer: The Department strongly supports a minimum level of funding to all the states, the District of Columbia, the Commonwealth of Puerto Rico, and the territories, which ensures baseline prevention, response and recovery capacities. It has become clear though that the formula currently being used for distribution of ODP grants, and partially defined within the USA PATRIOT Act of 2001, can be improved. The concept behind the PATRIOT Act's formula is valid: security needs to be improved everywhere, and the most protection is needed where the most people are located. But the PATRIOT Act formula fails to recognize that linear population increases do not equate to linear threat increases. Concentrations of critical infrastructure and politically attractive targets can tend to increase threat levels exponentially.

Indeed, the need to separate funds out for high-threat urban areas was recognized and addressed in both the Department's Fiscal Year 2003 Omnibus Appropriations Act and the Fiscal Year 2003 Emergency Wartime Supplemental Appropriations Act by separating funds out from the ODP formula grants. This same modification to the PATRIOT Act formula was carried forward in the DHS FY 04 Appropriations Act. We believe this ability to focus our funds on population and threat is both prudent and desirable. We further believe that this ability, as provided by the House and Senate Committees on Appropriations, sets the proper context for any discussions regarding a permanent change to our funding formula.

98. Representative Cox has introduced legislation, H.R. 3266, which would eliminate a minimum level of funds for each state and instead distribute homeland security funds only on the basis of threat risk and vulnerability. He has also proposed to provide funds to regions, instead of states. Do you believe that homeland security funding should be provided solely based on risk, threat, and vulnerability? Do you also believe that regions, instead of states should the primary recipient of homeland security funding?

Answer: The Department has come to realize the shortcomings of the funding formula under the USA PATRIOT Act, and appreciates Congressional interest and action to address those concerns. It is important that the Department have the ability to focus its funds on population and threat.

More specifically, "The Faster and Smarter Funding for First Responder Act" proposed by Representative Christopher Cox calls for the establishment of a State and Regional

Preparedness Grant Program to be administered by the Office of State and Local Coordination. According to the legislation, states and regions (multi-state or intra-state consortiums) may apply for grant funding for first responders.

The Department concurs with the Congressman's desire to deliver first responder grant funding in a more streamlined and expeditious manner. DHS currently works closely with our intergovernmental constituents to coordinate the distribution of grant funding to states and local communities throughout the nation. Just last week, the Department's Office of Domestic Preparedness delivered approximately $2.2 billion in first responder funding to state and local governments through an online "one-stop-shop" application process.

The delivery of grant funding through regional intra- or multi-state consortiums deserves further examination. As the Department continues to coordinate and integrate its programs throughout the nation, new and innovative approaches to disseminating homeland security funding is a priority in our effort to deliver effective and efficient services to our state and local partners.

99. The fiscal year 2004 Homeland Security Appropriations Bill directs the Office for Domestic Preparedness to use the Patriot Act formula to distribute their formula based grants. Does the Department intend on following this direction?

Answer: See answer to Question 97.

100. The national strategy describes the use of state homeland security task forces for DHS coordination.

- Should centralized state homeland security task forces remain the primary vehicles for DHS coordination?
- Is so, what are their strengths and weaknesses in fostering coordination at the state level? Local level?
- If DHS establishes guidelines for the roles and composition of the task forces, what should be the preliminary standards that might be proposed?
- If state task forces will not be the primary coordination vehicles, what should replace or complement them, and why?

Answer: I believe that the current system, which utilizes homeland security advisors in each state to build statewide strategic plans from the bottom up with local participation, is efficient. States should be given the discretion and flexibility to establish task forces that meet their needs and reflect their unique circumstances. We review each state's process throughout the state homeland security assessment and work to help ensure that they spend homeland security dollars as efficiently and effectively as possible.

101. Do you believe that the Office for Domestic Preparedness should work with the Information Analysis and Infrastructure Protection Directorate to measure threats posed to more rural states, such as agro-terrorism or remote border crossings and coastlines? If so, how should IAIP provide this advice and assistance to ODP?

Answer: When developing an overall threat picture, DHS/IAIP analyzes information from a number of sources. The system for receiving information from the Intelligence Community, TTIC and DHS components is described in the response to question 59. However, receiving information from state and local and private sector individuals is also a vital part of assessing threats and developing warning products. Threats posed to more rural states are a part of this process. Through ODP, as well as through other DHS Directorates such as Border and Transportation Security and the United States Coast Guard, IAIP is able to form a comprehensive domestic threat picture. Via warning and information products the threat assessment reaches those entities that may be affected by a given issue. These products are disseminated through the state and local officials, including the State Homeland Security Advisors and Governors, and the private sector.

The Office for Domestic Preparedness and the Information Analysis and Infrastructure Protection Directorate worked closely together to determine funding priorities for the Fiscal Year 2003 Urban Areas Security Initiative, and are currently working to finalize funding for the Fiscal Year 2004 Urban Areas Security Initiative. As you know, based on congressional direction in the Department's FY 2003 and FY 2004 appropriations act, this program focuses on high threat, high density urban areas. The Department recognizes the need for predominantly rural and agricultural areas to conduct similar analyses of threats and vulnerabilities to possible terrorist attacks. To meet this need, the Department significantly updated its State Homeland Security Assessment and Strategy (SHSAS) process to incorporate a suite of assessments focused on agricultural vulnerabilities and response capabilities to WMD incidents involving agricultural resources.

This optional agricultural assessment component was developed in coordination with the U.S. Department of Agriculture for state use, and addresses potential agricultural targets, agricultural planning factors, and current and desired agricultural response levels. There are also agricultural components included in the planning, organization, equipment, training, exercises, and technical assistance portions of the basic SHSAS process. Jurisdictions within the state that have substantial agricultural industry resources, activities, or enterprises, are encouraged to complete the agricultural component in addition to the basic assessment. States/jurisdictions that wish to complete the agricultural assessment are encouraged to establish an agricultural working group comprised of experts who understand the complexities of the agricultural industry.

The optional Agriculture Vulnerability Assessment provides an opportunity for states/jurisdictions to assess potential agricultural targets (through the evaluation of the target's level of visibility, criticality of the target, impact on the agricultural industry,

access by a potential threat element to the target, capacity of the agricultural facility, and the product distribution area). Once the Agricultural Vulnerability Assessment has been completed, a determination should be made regarding possible biological scenarios seen as a potential for the state/jurisdiction. Through the assessment, the state/jurisdiction is asked to evaluate the approximate number of animals/plants affected by the hypothetical biological incident. That estimated count represents a maximum need that ensures the state will have the information required for proper resource allocations to emergency responders. When completing this portion of the assessment, the agricultural working group should consider an attack against an agricultural facility, site, system, or special event that would produce animal death and/or plant contamination damage that would overwhelm the jurisdiction's agricultural emergency response capabilities, including any mutual aid agreements/assistance pacts.

The next step in the overall agricultural assessment is to examine the desired and current response capabilities of the first responders who will assist in the response to an agricultural incident. The purpose of conducting the agricultural capabilities and needs assessment is to assist states/jurisdictions in identifying agricultural planning, organization, equipment, training, and exercises they will need to safely and effectively respond to agricultural incidents.

All information collected through the agricultural assessment process (with the exception of sensitive threat information) will be submitted to ODP through a secure, web-based data collection tool. States will use the results from the agricultural assessment in completing the State Homeland Security Strategy, a blueprint for comprehensive planning for homeland security efforts that address the scope, nature, and extent of the challenge faced by emergency responders and that explain the state's strategy for utilizing state planning, organization, equipment, training, and exercise resources as well as may other resources available that will enhance efforts to increase prevention and response capabilities. As you know, states are required to provide completed state homeland security strategies to ODP for review by December 31, 2003 as a condition of receiving their Homeland Security Grant Program allocations.

102. Do you think the best way of providing grant funds to rural states to ensure a baseline level of protection is still through a minimum allocation of funding to each state?

Answer: As I noted previously, the Department strongly supports a minimum level of funding to all the states, the District of Columbia, the Commonwealth of Puerto Rico, and the territories. The minimum state funding levels serve to ensure baseline prevention, response, and recovery capacities, including those of rural areas within each of the states. It has become clear though that the formula currently being used for distribution of ODP grants, and partially defined within the USA PATRIOT Act of 2001, can be improved upon. The concept behind the PATRIOT Act's formula is valid: security needs to be improved everywhere, and the most protection is needed where the most people are located. Beyond that the Department is committed to working with Congress to ensure that more of the available grants are distributed on a risk formula.

Critical Infrastructure

103. In putting together state and local homeland security plans, state and local officials need to compile inventories of the critical infrastructure in their jurisdictions, assess the vulnerabilities of those infrastructures and develop plans for protecting those infrastructures. What is DHS doing, and what more will you do, to assist state and local governments in this effort? Does DHS share, or does it plan to share, its critical infrastructure inventory in a given jurisdiction with the officials of that jurisdiction so that officials at each level of government do not have to engage in duplicative efforts in identifying and assessing the vulnerabilities of such infrastructures, and to ensure that critical infrastructure protective strategies are coordinated? Does DHS systematically obtain and use information from states and localities about what those states and localities have already done to identify and protect critical infrastructures?

Answer: DHS recognizes that critical infrastructure protection is an "all hands effort" and that there needs to be a unified and coordinated approach taken in both the public and private sector and at all levels of government. To ensure that this happens, DHS, through its Information Analysis and Infrastructure Protection (IAIP) is now in the process of both writing and simultaneously implementing an operational plan to ensure there is a common protective framework and command and control among all of the stakeholders in the protective security arena. To support federal facilitation and local execution, DHS (IAIP) is deploying assets at the regional, state, and local levels. A few of the actions being taken include:

- DHS (IAIP) is now establishing, on a pilot basis, Security Augmentation Teams (SATs) that are drawn from municipal SWAT and other specialized disciplines to assist in writing protection plans for the most vulnerable sites in a given region and assist in enhancement of their protection.

- During Hurricane Isabel, DHS (IAIP) was prepared to deploy Protective Security Advisory Teams (PSATs) to the potential impact areas to identify areas that could be at risk of attack during that severe weather event. PSATs continue to be deployed on a weekly basis to assess and assist in the protection of sectors at high risk (e.g., chemical plants).

DHS is developing a program to assist state, local, and private asset owners to properly secure their respective assets. Regional training sessions have been conducted at those site DHS believed would benefit from immediate instruction. More sessions are planned.

As indicated above, it is DHS' goal to continue to expand and improve our means of direct liaisons with existing state and local bodies charged with conducting protective activities. DHS' information on infrastructure is based primarily on information provided by state governments, associations, and other sources. It is our intent to share this

information (to the maximum extent permitted under current security guidelines) to our partners in the states to ensure best utilization of our protective resources.

104. An estimated 85% of the United States' critical infrastructure – those systems on which so much of our economy and daily life depends – is privately owned. There is a danger, however that private businesses may not be taking adequate steps to safeguard this infrastructure. This might be due to a number of factors, including that individual businesses may not believe their facilities are at risk – a survey by the Council on Competitiveness, for example, found that 92% of surveyed executives of the nation's largest companies did not see their companies as potential terrorism targets – and that businesses may not have adequate incentives to protect against an attack that is, at any one point, unlikely and where some of the costs of the attack are borne by those other than the property owner (where, for example, individuals are injured by the malicious use of hazardous materials stolen from a private facility or in the case of the symbolic loss to the nation of an important commercial landmark). What will you do to ensure that privately owned critical infrastructure is being adequately protected? What criteria will you use to evaluate whether private efforts to protect such infrastructure are adequate or whether additional efforts, including regulations, are needed? Applying these standards, in what sectors do you think additional efforts, including regulations, may be needed?

Answer: DHS will continue pursuing a policy of information sharing with the private sector and actively promote awareness of security measures among industry leaders. DHS will promote the use of self-assessments for security and vulnerability testing by the private sector. The criteria for assessing the adequacy of private sector security efforts will be based on industry based best security practices along with expert developed security standards. IAIP in concert with professional security and vulnerability experts is developing self-assessment tools for private critical assets owners to assess the security and vulnerabilities of their assets. As indicate above, IAIP is also developing General Protection Plans as the basis for these self-assessments.

I do not feel that additional regulation is needed at this time. It is our view that the "market" is best suited to reward those sectors and assets owners that implement the appropriate level of security measures given the associated level of risk. The owners and operators on these facilities are the best motivated to ensure that their property and personnel are protected.

Privacy

105. The Department of Homeland Security is the first department or agency to have a codified privacy officer; her statutory responsibilities include assuring compliance with the Privacy Act and "assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information."

- What will you do to ensure the independence of the Privacy Officer?

Answer: Secretary Ridge has pledged, and I will echo, that the Department's leadership will not in any way interfere with the privacy officer's judgment or findings relating to a particular program or a particular individual's complaints. I, in my work at TSA, have already worked closely with our privacy officer, Nuala O'Connor Kelly, and will continue to support her office's important work towards ensuring individual privacy. The privacy office is represented, including at the most senior levels, in all policy discussions relating to the collection and use of personal information by the Department. Further, the headquarters privacy office is supported by the work of Privacy Act and Freedom of Information Act officers throughout the Department--over 300 personnel who support this office's mission.

- What steps does the Department need to take to ensure that the Privacy Officer's autonomy and ability to influence Department policy are institutionalized?

Answer: The Privacy Officer's autonomy appears to be well established, particularly under subsection (5) of Section 222 of the Homeland Security Act, which provides a direct reporting relationship between the privacy office and Congress--not a reporting relationship through the Secretary or other Departmental official--on controls, complaints, and other matters handled by the Privacy Office. The inclusion of the Privacy Officer in the Department's Investment Review Board also provides a formal oversight mechanism for the Privacy Office. Steps may need to be taken to formalize and institutionalize the Privacy Office's budget and staffing, to ensure that all parts of the Department are adequately monitored by the Privacy Office.

106. The development of data-mining initiatives by the FBI, TSA, and DARPA has raised concerns about privacy. How should the Department address those concerns when developing data mining initiatives?

Answer: Through the inclusion of the Privacy Office in the development of new programs and policies involving the collection of personal data, we believe that the Department can create responsible and meaningful protocols surrounding the use of personal information, including the collection of personal data from the individual or from private sector companies. The Privacy Office is already working collaboratively with private-sector think tanks, academicians, and advocacy groups to create such frameworks, while still achieving the mission of the Department.

IV. Relations with Congress

107. Do you agree without reservation to respond to any reasonable summons to appear and testify before any duly constituted committee of the Congress if you are confirmed?

Answer: I do so agree.

108. Do you agree without reservation to reply to any reasonable request for information from any duly constituted committee of the Congress if you are confirmed?

Answer: I do so agree.

V. Assistance

109. Are these answers your own? Have you consulted with DHS or any other interested parties? If so, please indicate which entities.

Answer: These answers are my own. Normal preconfirmation consultation with the White House Personnel Office, the Office of Government Ethics and the respective Counsels at DHS and TSA have been conducted.

AFFIDAVIT

I, James M. Loy, being duly sworn, hereby state that I have read and signed the foregoing Statement on Pre-hearing Questions and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

James M. Loy

Subscribed and sworn before me this 17th day of November, 2003.

Victor L. Martini
Notary Public

Pre-hearing Questions Submitted by
Senator Susan M. Collins,
Chairman, Senate Committee on Governmental Affairs
for the Nomination of James M. Loy
to be Deputy Secretary of Department of Homeland Security

1. **The Homeland Security Advanced Research Projects Agency (HSARPA) is a component of the Science and Technology Directorate. HSARPA is modeled after the Defense Advanced Research Projects Agency (DARPA) which is administered in the Department of Defense. In recent months significant privacy concerns have been raised about the development of the Total Information Awareness Project by DARPA. What are the challenges in ensuring that the development of HSARPA projects does not raise legitimate concerns about the privacy of American citizens?**

   Answer: I appreciate your concerns, which are shared by the Director of HSARPA, Dr. Bolka, and his staff. Moreover, the Department has both a Privacy Officer and an Office of Civil Rights and Civil Liberties to monitor and advise departmental officials on potential or actual implications for privacy rights that may result from our research and how it is conducted.

   The research challenge is to balance our citizens' high expectations for privacy against their equally high demand for protection against terrorist attack.

   We are aware of the issue, we are sensitive to its importance, and our HSARPA leaders will ensure that our research progresses in a way that is compatible with legitimate privacy concerns.

2. **Certain language in the HSA might be interpreted to require HSARPA to emulate specific DARPA programs. What do you see as the major differences between the overall goals of HSARPA and those of DARPA and how will the two entities work together?**

   Answer: DHS does not interpret the Homeland Security Act to require or direct HSARPA to emulate any DARPA programs.

   While it is true that HSARPA was modeled on DARPA, HSARPA has a significantly different in function. Unlike DARPA, approximately 85% of HSARPA's budget will be applied against identified, prioritized DHS requirements. Only a small portion of its budget (the remaining 10-15%) will emulate the DARPA model of path-breaking, revolutionary research – research that may lead to dramatically greater advantages over terrorists and their methods. Although it is the smaller part of the HSARPA budget, the ability to

investigate potential technology breakthroughs is absolutely essential to our nation's preparedness. This is the "outside-the-box" technology investment.

In both organizations a highly competent Program Manager is accountable for each program's results and gives it active, technical guidance. Also, the program execution is tailored to the individual goals of that program. Further, Congress provided both organizations with a full range of flexible contracting methods and the authority to hire the talented personnel needed.

However, in some very important ways, our requirements differ from those of other federal agencies. Although DHS, DoD and even DOE share a common technology base in some areas, the DHS applications, users, and operational environments are significantly different and require different engineering solutions. Systems we develop must address whole regions of varying capabilities, governments, vulnerabilities and legacy systems.

Affordability is an overriding concern for us. If government agencies, agents and first responders cannot buy the technology developed, then the added capability required is not achieved. Finally, DHS cannot mandate a Federal technology solution for first responders.

Under the Homeland Security Act, DHS is required to coordinate with DARPA and other relevant research agencies, and HSARPA was given the authority to run joint programs with DARPA. This is critical, because it encourages the exchange of research results for the mutual benefit of both departments. Defending, protecting, and securing the Homeland require that every single federal research dollar be spent wisely and to maximum effect.

3. **Earlier this year, I sent a letter to BCIS Director Aguirre asking him to consider adding a BCIS office in Bangor, Maine. As a result of the creation of the Department and the reorganization of the Immigration and Naturalization Service, virtually all immigration services in Maine were transferred to the BCIS office in South Portland, ME, which is some 350 miles from the state's northern border crossing at Madawaska, ME. Maine's land border stations see a regular influx of foreign visitors and workers every year and many of these areas are also home to a number of businesses, major medical facilities and education institutions. As a result, there are many students, researchers and foreign workers who need immigration services on a regular basis. Having the main BCIS office in South Portland is not practical and is inefficient. Can I get your assurance that you will work with me and Director Aguirre to address this issue and find some way for the BCIS to offer services for all of Maine in a more practical and effective manner, preferably through the establishment of a BCIS office in Bangor?**

Answer: At this time the immigration inspection station in Bangor, Maine is operated by Customs and Border Protection (CBP), a bureau within the Department of Homeland Security (DHS). These CBP immigration inspectors are able to answer basic questions concerning immigration issues; however, individuals must travel to the DHS U.S. Citizenship and Immigration Services (CIS) District Office in South Portland, Maine to receive complete assistance regarding Adoptions, Advance Parole, Appointments, Bonds, Canadian Border Boat Landing Permit, Case Status, Change of Address, Citizenship Ceremonies, Deferred Inspection, Designated Civil Surgeons, Emergency Travel Authorization, Employment Authorization Documents (EAD), Employer-related Immigration Matters, Fingerprints, Forms, Freedom of Information Act (FOIA), Immigration Court, Naturalization Information, Orphan Petitions, and Travel Documents. Mailing and Street Address: U.S. CIS Portland, Maine District Office, 176 Gannett Drive, So. Portland, ME 04106.

We recognize that in Maine, some people have to travel a very long distance to get to a CIS office; however, based upon a workload analysis, opening an office Bangor, Maine would not be feasible. The leadership staff at CIS headquarters is constantly evaluating workloads and trends. The District Director in Portland, Maine is looking into whether a circuit ride or some other arrangements could be made to serve those customers who would otherwise have to travel hundreds of miles to a CIS office.

As Deputy Secretary, I would plan to work with CIS Director Eduardo Aguirre, and CBP Commissioner Robert Bonner together to determine the most efficient way to offer immigration services in all parts of Maine.

In support of the DHS overall mission, the immediate priorities of the new U.S. Citizenship and Immigration Services (CIS) are to promote national security, continue to eliminate immigration adjudications backlogs, and implement solutions for improving immigration customer services. CIS will continue efforts to fundamentally transform and improve the delivery of immigration and citizenship services.

4. **As you know, S.1245 directs the Secretary to set aside ten percent of the appropriated grant program funds for high-threat urban areas. Some have suggested that DHS retain the regional metropolitan area approach in the development and implementation of the high threat urban area grant program by core cities, counties, contiguous jurisdictions, and mutual aid partners, but provide funding directly to these local governments.**

This approach would promote coordination between the regional governments and the State homeland security plan to enhance mutual aid agreements, interoperability of the communications systems, and coordinated emergency planning efforts. At the same time, this approach would provide high threat funding directly to the local governments in those

affected areas and make sure those first responders in high threat areas receive funding on an expedited basis. Would you support modifying the current approach to retain the regional structure but provide funding directly to the local governments included in the high threat region?

Answer: The Department developed the Urban Areas Security Initiative to address the unique security challenge of high threat and high-density urban areas. We believe that the design of the program is the most effective and efficient method to ensure that there is coordination and communication in the high threat urban areas. By providing funds through the State, while at the same time requiring the state in certain cases to distribute those funds to a high threat area or region, we continue to encourage state wide and regional planning efforts. If we provide direct funding to specific localities, we run the risk of fragmenting our preparedness efforts.

Further more this approach has been validated by the positive feedback we have received from jurisdictions participating in the program from its early implementation.

5. **Senator Collins believes that more funding should be based on risk, threat, and vulnerability. S.1245 would allocate more than 60 percent on risk, threat and vulnerability. Do you support adjusting homeland security funding based on threat instead of population?**

Answer: The Department is supportive of working with Congress on passing more Homeland Security dollars on threat while at the same time supporting the idea that all communities need some base level of funding to make their neighborhoods more secure.

6. **There have been reports circulating regarding an Administration proposal to require Canadian citizens to carry and show passports when entering the United States. Residents and businesses on both sides of the border depend on each other. In addition, many families have relatives on both sides of the border and the ease of crossing has always enabled families to maintain strong ties. Any action taken by the U.S. that hinders that relationship could damage the economies of Maine and other border states as well as established cultures. When crafting border policies, a balance between security and commerce must be sought. How is the Department addressing the issue of Canadian citizens who travel to the United States and what are the possible options? What is the Department's preferred option?**

- **How will the US VISIT program be applied to Canadian citizens?**

Answer: Under current policy, most Canadian citizens are not subject to the provisions of US-VISIT. Canadians who are required to have visas to travel to the United States are an exception and will be subject to US-VISIT.

- **What can United States citizens expect in the future when traveling to Canada?**

Answer: DHS is working closely with Secretary Powell's staff on a series of important initiatives to strengthen our ability to ascertain the identity of persons entering our country and improve the security of travel to our shores. Similarly, we began work with the Government of Canada immediately following the tragic events of September 11th on measures to enhance our mutual security -- both the security of our populations and shared infrastructure as well as the security of our integrated economies. In December 2001, we signed the U.S.-Canada "Smart Border" plan that lays out 30 concrete steps we are taking to improve security. The NEXUS and FAST programs, designed to facilitate cross-border visits and commercial activity for known, low-risk travelers, are wonderful illustrations of the cooperation between our two Governments. Together with the Canadian Customs and Immigration officials, DHS has expanded these "smart lanes" from the Pacific Northwest to the east coast. We look to local border communities for support of these voluntary programs and expect enrollment to increase as frequent travelers recognize the benefits of access to these special lanes at busy ports-of-entry. We are also working with Canadian officials to pilot a NEXUS Air program in the coming year, recognizing that many of our citizens travel frequently by air to and from Canada.

The issue of whether to require passports for travel across the U.S.- Canada border is particularly complex and significant in several ways. Such a proposal would enhance security by addressing a vulnerability in screening individuals at our ports-of-entry yet would necessitate a philosophical shift in the way Canadian and U.S. citizens think of our common border and may have a potential economic effect on cross-border commercial activity. Department of State and DHS are in the beginning stages of considering this far-reaching issue. We will work with Members and Committees as our examination of this proposal progresses.

Additional Pre-Hearing Questions
From Senator Joe Lieberman
For the Nomination of James M. Loy to be
Deputy Secretary of the Department of Homeland Security

National Strategy

1. Writing in the November issue of *American Prospect*, terrorism expert Juliette Kayyem complains that the *National Strategy for Homeland Security* is a "catalog of conventional wisdom" that fails to set priorities and provide clear guidance. Others have noted that the document lacks deadlines or other firm benchmarks to hold the government accountable.

   - Do you believe the Strategy provides sufficient guidance for the nation's homeland security efforts? Why or why not?

     Answer: I believe the National Strategy does what it is designed to. This document is an overarching statement of intent by this President. It prescribes his concern and initiates the work, both conceptual and practical, that must be done to secure our Homeland. Those of us responsible for that work must both challenge conventional wisdom and recognize the very real differences in the security environment we live in post 9/11. DHS is leading the way with that work to include real deadlines and benchmarks in hundreds of areas of challenge.

     DHS is building its Strategic Plan that will both interpret the National Strategy and outline the vision the Administration has for securing the Homeland. That document will provide the strategic goals, objectives, activities expected with full attention to timelines and accountability. Our goal will be to articulate for the country and the DHS workforce the cohesive plan necessary to accomplish the mandates articulated in both the National Strategy and the Homeland Security Act.

   - Are there plans to update the Strategy? If so, when? If not, why not?

     Answer: DHS is building the Strategic Plan that will both interpret the National Strategy and outline the vision the Administration has for securing the Homeland. That document will provide the strategic goals, objectives, activities expected with full attention to timelines and accountability. Our goal will be to articulate for the country and the DHS workforce the cohesive plan necessary to accomplish the mandates articulated in both the National Strategy and the Homeland Security Act.

Human Resources

2. What are your views on the value of collective bargaining at DHS? For example, do you believe that protection of the right to bargain helps hold agencies accountable for upholding the

merit system? Does such protection safeguard the public interest and contribute to the effective conduct of public business?

On the other hand, are you aware of any instances in which collective bargaining has jeopardized national security or the fight against terrorism? In the case of the screeners at TSA, are you aware of any instances in which collective bargaining would have jeopardized national security, had the screeners had such rights?

> **Answer:** Ultimately, it is the responsibility of the leadership in every Department and agency to protect the merit principles and create a work environment where employees can effectively perform their duties. That responsibility can be enhanced by appropriate collective bargaining. Collective bargaining can also contribute to the effective conduct of public business.

3. Before the creation of the CBP officer position as part of the "One Face at the Border Initiative," the legacy Customs, INS, and APHIS inspectors underwent extensive specialized training in their respective areas of expertise. How will the new officers under the "One Face at the Border" program be adequately trained to enable them to make our borders secure?

> **Answer:** The Homeland Security Act merged these different specialized inspection workforces to carry out the priority mission of preventing terrorists and instruments of terrorism from entering the United States while facilitating the flow of legitimate trade and travel, and to perform the traditional missions of the three legacy agencies. "One Face at the Border" establishes one-stop processing, a single officer to interact with the traveling public and trade community at the nation's ports of entry. The CBP Officer is a sound concept because it capitalizes on the skills and competencies that are common to the occupations: observation, analysis, risk-assessment, interviewing, examination, etc. The legacy inspectors became specialty experts by learning, interpreting and applying the laws and regulations applicable to their inspectional work; they will now be learning new laws and regulations, and developing new areas of expertise. Specialized Agriculture expertise must be retained to carry out duties that require undergraduate education in biological sciences.

Critical Infrastructure

4. Since at least 1998, when President Clinton issued Presidential Decision Directive 63, the need to systematically identify, assess and protect our nation's critical infrastructure has been identified an important governmental priority. Nonetheless, this mission appears to remain woefully incomplete. With respect to each of the thirteen sectors of critical infrastructure and five categories of key assets identified in the Administration's *National Strategy for Homeland Security* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, what is the current status of the Department's efforts to (a) compile a comprehensive inventory of all critical infrastructure and key assets in the sector; (b) conduct vulnerability assessments of those infrastructures and assets; (c) conduct risk assessments of the infrastructures and assets; (d) develop and implement protective strategies for those infrastructures and assets?

As Administrator of TSA, what specifically have you done to ensure that critical infrastructure in the transportation sector is inventoried, its vulnerabilities assessed, and measures taken to protect the infrastructure? As Deputy Secretary, what will you do to ensure that the requisite inventories and assessments are completed expeditiously and that our nation's critical infrastructure is adequately protected?

Answer: We are evaluating transportation infrastructure assets in all modes of transportation utilizing TSA criticality model (incorporating IAIP tenets) to identify national critical infrastructure. To date we have evaluated over 420 assets, and we are moving as expeditiously as possible to complete all the evaluations. Evaluations are being done in concert with DOT's modal administrators and industry representatives.

CAPPS

5. According to a TSA fact sheet released September 29, 2003, "CAPPS II will authenticate the identity of passengers by checking the passenger name record - including full name, home address, telephone number and date of birth - against commercial databases. In addition, a risk assessment will be done by checking passenger names against government databases."

- How difficult would it be for a terrorist to acquire over the Internet or through other means the four personal data elements (name, home address, telephone number and date of birth) of law-abiding Americans who are not likely to be assigned yellow or red ratings by the CAPPS II system?

  Answer: Under the current system, a person can fly after having someone only quickly view their photo identification and comparing it with the name on the ticket. With CAPPS II, the four PNR data elements start a process of authentication, which validates and verifies information provided by the individual. With only these four data items, a terrorist would not necessarily receive a high enough authentication and risk assessment score to be assigned a green rating by the CAPPS II system.

- How difficult would it be for a terrorist to acquire or fabricate false identification convincing enough to fool airport personnel?

  Answer: Fraudulent documents are clearly a major problem in protecting the Nation's security. Currently at our airports, personnel view photo-identification, but have limited methods of checking on its validity. Law enforcement agencies are, of course, currently working on the problem.

  CAPPS II is designed to significantly increase – exponentially increase – the capacity of the government to know that the person who is traveling is who he or she says they are. Providing airport personnel with the additional assets of advanced information-based authentication makes it far more difficult to fool anyone than is currently possible.

- How easy would it be for a terrorist to entirely evade the CAPPS II system by assuming another person's identity with the aid of false identification? Does this suggest a vulnerability in the CAPPS II approach? If so, what is TSA doing to address the vulnerability? If not, why not?

  Answer: Identity theft is clearly a problem for law enforcement, counter-terrorism, and commercial fraud detection. In the absence of a national, biometrically-based identity card, CAPPS II represents the most robust protection. Unlike current approaches, CAPPS II runs on a government, rather than a private sector, platform. It is threat-based, which allows real-time intelligence information to be shared and delivered to those who need it most. And its data systems and protections match state-of-the-art security requirements. CAPPS II also has built-in privacy protections, and is designed to enhance the commercial stability of the airline industry by reducing vulnerabilities and their potential impacts.

  As described above, under the current system, a person can fly after having someone only quickly view their photo identification and comparing it with the name on the ticket. With CAPPS II, the four PNR data elements start a process of authentication, which validates and verifies information provided by the individual. With only these four data items, a terrorist would not necessarily receive a high enough authentication and risk assessment score to be assigned a green rating by the CAPPS II system.

Border Security / Immigration

6. The "Agricultural Job Opportunity, Benefits, and Security Act", S. 1645, bipartisan legislation introduced by Senators Craig and Kennedy and co-sponsored by 39 other senators, would allow undocumented immigrant agricultural workers who have resided in the U.S. peacefully for a defined period of time to apply for legal permanent residency (LPR) status. The DREAM Act, S.1545, bipartisan legislation introduced by Senators Hatch and Durbin and co-sponsored by 40 other senators, would offer similar relief to high school graduates who had been brought into the country as children. Many in Congress also advocate a broader earned legalization program for law-abiding immigrants who pass background checks, as well as a new temporary work visa to channel future immigrants into legal jobs and lawful status. Many proponents of these proposals argue that they would enhance our homeland security, as they would regularize a large number of undocumented immigrants who do not pose a danger to the community, allowing law enforcement to concentrate more effectively on the remaining foreign nationals residing unlawfully in the country.

- Do you believe that earned legalization and work visa programs of the type described above could enhance our security? Why or why not?

- What is the Department of Homeland Security doing, and what should it be doing, to assess the security implications of earned legalization programs?

Answer: The Department is interested in making our migration policies safe, orderly, humane, and legal, and policies that match willing workers with willing employers make sense. However, as with all legislation, we will have to review the proposals carefully. Should I be confirmed as Deputy Secretary, I look forward to conducting this review.

7. There are an estimated eight million undocumented immigrants living in the United States. Of these, more than three hundred thousand have absconded from final deportation orders, and ten of thousands are convicted felons subject to deportation who were nevertheless released from state and local prisons.

- Given the large numbers of undocumented immigrants living in the United States, how should the Department of Homeland Security set its enforcement priorities? Do you agree that the Department needs to make choices in how it allocates its limited enforcement resources?

- To what extent should the Department pursue undocumented immigrants who have not absconded from final deportation orders or broken the law? What is the value of enforcement against this population?

- Do you believe the Department should take legal action against employers of undocumented immigrants? How, in what circumstances, and to what extent?

Answer: Our priorities are to enhance national security; promote public safety; disrupt and dismantle the financial infrastructures of organizations that would harm the United States; and identify and remove individuals, especially criminals and others who pose threats to the national security and public safety, who are unlawfully present in the United States.

Resources permitting, all violations of our immigration laws should be addressed. Given resource constraints within DHS as well as with DOJ, priority must be given to the most serious offenses. As resources increase, enforcement activities should see a corresponding increase. Bringing integrity to our immigration system is a very important goal that is directly related to fighting terrorism. The more aliens unlawfully present in the United States, the more difficult it is to identify and locate those aliens who wish to do us harm.

BICE will enforce the criminal provisions of federal statutes and administrative provisions of the Immigration and Nationality Act. We will investigate and refer for prosecution violations including those employers exploiting foreign nationals either physically or economically. Consistent with our mission to secure the homeland, we are focusing our resources on employers with workers who have access to sensitive

and critical infrastructure and high profile events that may be targeted by terrorists. Again, as resources increase, employment enforcement activities should see a corresponding increase.

8. A recent AP investigation, published on November 2, 2003, reported that "a crackdown along the U.S.-Mexico border designed to prevent terrorists from entering the United States hasn't stopped even one known militant from slipping into America since September 11." The AP reported that the crackdown instead had "slowed trade, snarled traffic and cost American taxpayers millions, perhaps billions, of dollars, while hundreds of migrants have died trying to evade the growing army of border authorities." The article quoted a Border Patrol agent as saying a terrorist would be more likely to go to the Northern Border "where we don't have the resources to stop them." The article also noted that the September 11 hijackers had entered the United States on visas.

- What is your response to the issues raised by this report?

  Answer: The enforcement operations along both the Northern and Southern borders have stopped known militants from entering the United States. Each day, Customs and Border Protection stops dozens of passengers from entering the United States many of them attempting to gain access to the U.S. using false documents or in many cases attempting to gain entry via illegal means between our ports of entry. Many of these individuals are associated with extremist groups and by denying them entry to the U.S. we are effectively enhancing the security of the U.S. Customs Service.

  The most obvious and readily available threats are the ports of entry and the urban areas where illegal aliens more easily blend into the community and more easily access critical infrastructure and routes of egress away from the border. As a result of an increased application of enforcement resources (i.e., sensors, remote video surveillance cameras, aircraft, intelligence efforts, 1000 agents to be deployed along the northern border, etc) in these critical areas, smugglers have indeed chosen to move aliens through more remote and hostile terrain. However, border enforcement actions are expanding into more remote border areas in an effort to make the border more secure and safe.

- Is there evidence that terrorists might try to enter the United States across the southern border from Mexico?

  Answer: The evidence that is before us today indicates that terrorists are determined in their pursuits. No stretch of border can be ruled out as a potential crossing place for terrorists. Specifically, there is significant evidence that both the Southwest border of the U.S. and the Northern border of the U.S. are known to groups such as Al Qaeda as possible crossing points into the U.S. Each presents certain opportunities and vulnerabilities; especially those associated with the normal flow of large volumes of commerce and trade. However, Customs and

Border Protection is addressing these issues on a daily basis through intelligence based operations, intensive targeting of all conveyances, layered inspection approaches, and enforcement operations that seek to deter and disrupt any potential operations.

- Do you agree that a well-funded terrorist would be able to enter the United States with much less risk across the Northern border? If so, what should be done about that problem?

  Answer: DHS and its components have been working very closely with both Canada and Mexico on rigorous and aggressive anti terrorism initiatives and significant progress has been make to improve border security across the board. While the actual inspectional procedures at the ports of entry may differ between the northern and southern borders, reflecting differences in regulations governing entry documentation, the inspection process itself does not. A CBP officer carefully reviews each application for admission; that officer must be fully satisfied that the applicant is entitled to enter the United States.

  Between the ports of entry, each border environment (north and south) poses challenges to the illegal entrant while at the same time providing potential opportunities for entry. For example, the volume of illegal alien traffic on the southern border could provide better access, cover, and concealment for potential terrorists attempting to illegally enter the country. The northern border on the other hand, though less heavily patrolled, is more remote, and the illegal alien traffic levels provide less opportunity for potential terrorists to blend in. Also, the Canadian government provides a greater law enforcement presence along our northern border, and the flow of shared information regarding border activity is greater. To further improve our capabilities on the northern border, Border Patrol is in the process of increasing our technology and aircraft in that area, and his targeted the northern border for a total of 1000 Border Patrol Agents by the end of the year.

- What do you believe are the greatest vulnerabilities at present in our efforts to keep terrorists from entering the country? How should we be addressing those vulnerabilities?

  Answer: There is no such thing as perfect security and it is certainly possible that a terrorist or someone intent on committing an act of violence could cross into the United States. Since 9/11 though, the cooperative work with the Department and its relationships with other agencies in the law enforcement and intelligence community makes this likelihood much less of a certainty. Moreover, there is documented evidence that Al Qaeda has been deterred through the security efforts at our border and that access to the United States is a more complicated and dangerous issue for potential terrorists. Many of the current threats that we are now examining have to do with Al Qaeda and other groups evolving their

strategies to defeat our border, airport, and other security procedures implemented successfully since 9/11.

CBP is constantly reviewing its procedures and operations to address the terrorist threat by providing the most up to date information to our line officers and developing additional training materials for them. As the intelligence community continues to provide better information to our inspectors, the vulnerabilities to our borders will become more manageable.

TSA

9. Do you support continued federalization of aviation passenger and baggage screening operations? Will you work to maintain TSA's current role in screening passengers and baggage? If not, please explain.

Answer: First, to my knowledge, a policy decision by the Administration on federalization versus privatization of the screening work force has not been made at this time. However, the Aviation Transportation Security Act does require TSA to enable airports to apply, starting next November 19, for private contractor screeners in place of Federal screeners, and TSA intends to be prepared to ensure effective security with either private contractor screeners or Federal screeners.

In the interests of being prepared for any eventuality, TSA is now in the early stages of developing a potential process for this "opt out" application program and is reaching out to public and private sector stakeholders for input and guidance. In addition, TSA is in the process of developing and executing a performance evaluation of the private contractor screening pilot program. This evaluation will serve as an input into our approach on privatization. For example, we intend to fully understand the potential impact on security performance, if any, posed by private contractor screeners.

Regardless of the eventual direction taken by the Administration and the Congress with regard to privatization, TSA seeks to maintain effective security and be an effective steward of taxpayer funds. With or without Federal screeners, TSA will maintain a strong role in screening passengers and baggage. This role may not always be an *operational* one, where TSA actually operates checkpoints as we do today, but it will certainly be, at a minimum, one of regulation and oversight. And given that airports are able to apply for opt-out *starting in* November 2004, it will be an operational role *for the near future.*

Regardless of the direction taken by the Administration and Congress, I will work to leverage all the tremendous work that TSA has completed and the knowledge that TSA has accumulated since federalization.

10. Under the provisions of the Aviation and Transportation Security Act (ATSA), TSA is implementing five pilot programs under which selected airports may utilize private companies to conduct aviation passenger and baggage screening. These programs must be evaluated by

November 2004, when ATSA allows other airports to request permission to enter into similar contracts for screening.

- What criteria and performance measures is TSA using to compare the pilot programs to TSA's own passenger and baggage screening operations?

  Answer: To ensure objectivity, TSA has retained an outside evaluator and is in the process of developing and executing a performance evaluation for this program, with the intent of examining private screening pilot program results in the areas of security effectiveness, financial efficiency, customer / stakeholder satisfaction. The specific metrics and criteria have not yet been finalized. TSA anticipates having an initial evaluation model for internal review by early December.

- Is TSA maintaining performance data that will allow a reliable comparison of these two programs? If so, please describe.

  Answer: TSA will have valid data that can be used effectively for the performance evaluation. The outside evaluators conducting the performance evaluation have met with TSA's internal groups to leverage currently available data is available and to understand any limitations it may have. Data sets that are available and are likely to be part of the evaluation in some manner include:

  Security effectiveness:
  - Threat Image Project (TIP) results;
  - Results of annual recertification tests;
  - Employee attrition statistics;
  - Covert testing results; and
  - Number & type of prohibited items surrendered at checkpoints

  Customer / stakeholder satisfaction:
  - Customer intercept surveys;
  - Reported complaints and compliments;
  - Customer wait times; and
  - Number of property claims per 1,000 passengers

  Financial efficiency:
  - Financial reports from TSA's financial systems, and
  - Contracts and invoices

  As we move deeper into the evaluation process, the outside evaluator will be looking at these data sources and more, and will apply proven, statistically sound techniques to derive meaningful evaluations.

11. According to a December 2002 GAO report, "terrorist events around the world have shown that mass transit systems, like other modes of transportation, are often targets of attack.

For example, roughly one-third of terrorist attacks worldwide target transportation systems, and transit systems are the mode most commonly attacked." *(Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges*, GAO-03-263.) GAO's report stated that "insufficient funding is the most significant challenge in making ... transit systems as safe and secure as possible" and estimated that the total cost of identified security improvements for eight transit agencies visited by GAO was roughly $711 million, with the price of securing all the nation's transit systems potentially reaching into the billions of dollars. The *Wall Street Journal* has reported that transit agencies across the country are strapped by tight budgets and have been unable to take many of the actions they feel are needed to improve security. ("Transit Agencies Seek to Boost Subway Security - Tight Budgets Put Limits on Local Efforts to Guard Against Terrorist Attack," *Wall Street Journal,* May 28, 2003.) Although DHS this summer selected the 20 largest transit agencies to receive $65 million in security grants, this amount will not provide the help transit officials say they need.

- What actions is DHS taking to secure:
  - subways
  - buses
  - commuter and light rail
  - ferries

- How will DHS coordinate with state, local and regional authorities to improve mass transit security and what role do you expect state, local and regional authorities to play?

- Has the Administration established standards or best practices for transit agencies to follow in improving security? If not, when will such guidance be available?

Answer: DHS intends to establish national standards for mass transit. We are sharing threat information with transit authorities. DHS is actively pursuing new technology and methodologies to protect mass transit systems. The Administration is currently developing a threat and vulnerability assessment model that will go beyond the scope of existing assessments to further define the risks associated with the nation's transit systems.

DHS is also coordinating with the Federal Transit Administration, the American Public Transportation Association, the Community Transportation Association of America, the Amalgamated Transit Union, and other stakeholders to harden the nation's transit system.

As an example of this coordinated approach, DHS and the Federal Transit Administration co-sponsored a security roundtable to address current transit security issues. Participants included personnel from 30 of the nation's largest transit security/police chiefs from across the country. Topics discussed included transit intelligence, threats and vulnerabilities and emerging transit security technologies.

12. In legislation reported out in the 107th Congress, the Senate Commerce Committee identified a series of significant enhancements necessary to improve rail security, including infrastructure security improvements, such as the protection of tunnels, bridges and other rail facilities; rail equipment security, including improved communications, surveillance, and detection equipment; and system-wide security operations, such as hiring and training additional investigative and patrol personnel. The Committee also sought to authorize funds for a pilot program to provide random screening of passengers and baggage at certain major Amtrak stations and for a study of security and safety at stations served by Amtrak.

- What action, if any, is DHS taking to address:
  - rail infrastructure security improvements
  - rail equipment security
  - system-wide rail security operations
  - random screening of rail passengers and baggage
  - security and safety at stations served by Amtrak

- Has DHS sought funding to address rail security, and if not, what is the Administration's timetable for making improvements in rail security?

Answer: DHS is working with the Federal Railroad Administration, Association of American Railroads, governmental, and industry stakeholders to establish national standards, develop security plans, better assess security vulnerabilities and identify needed security enhancements to the rail system and related infrastructure.

TSA is assessing vulnerability and critical infrastructure in developing standards to ensure an acceptable level of risk.

For example, TSA and FRA in partnership with Amtrak is developing a passenger and baggage-screening prototype for a selected station on the Northeast Corridor. The results of the prototype will be used to determine the impact to operations and security enhancement in a rail environment.

13. TSA reduced its screener workforce this year by a total of 6000 positions. The screeners affected had completed the TSA screener training and were deployed in airports across the country to screen passengers and baggage.

- How many screeners whose positions were terminated would have been qualified to remain on the TSA workforce if this reduction did not occur?

  Answer: By the end of the fiscal year, TSA had reduced the screener workforce by nearly 7,800 screeners, of which about 5,200 remained qualified.

- How much did it cost TSA to hire and train these employees?

  Answer: It cost TSA about $57 million to hire and train the 5,200 screeners.

- How many such screeners worked in airports that handle air cargo shipments on passenger aircraft? Is air cargo currently being screened for possible explosives in those airports?

  Answers: Air cargo moves on passenger aircraft operated by all the major airlines in the country. The airlines have assured us repeatedly that they consider opportunities to transport air cargo vital to their economic survival, and as a result they compete with one another for these opportunities. Consequently, although we do not have specific statistics on this point, 44 airports handle 95% of air cargo volume. Recognizing the importance of this manner of cargo transport, both in terms of security and in terms of the economic viability of the airlines, TSA has taken steps to restrict the type of air cargo that can be loaded onto passenger aircraft. Currently, only air cargo from known shippers and certain U.S. Mail are eligible for transport on passenger aircraft. Further restrictions are being (or were recently) implemented that we prefer not to discuss in open session, further enhancing the security of air cargo shipped aboard passenger airline aircraft.

  TSA screens cargo transported on passenger aircraft via TSA's Known Shipper program. Under this program, the air carriers and indirect air carriers that accept the shipment from the shipper must ensure the shipper's suitability based on the Known Shipper requirements established by TSA.

- TSA announced that some screeners who might otherwise lose their jobs would be given an opportunity to apply for transfer to airports that need additional screeners for passenger and baggage duties. Apart from this plan, did TSA consider redeploying screeners whose positions are being terminated to other needed tasks, such as screening air cargo, in lieu of eliminating these positions? If not, why not?

  Answer: Redeployment was not an option, as the FY 2003 funding level did not support maintaining the TSA workforce at this level regardless of screening activity performed.

14. A June 22, 2003 article in the *Washington Post*, "Airport Security Remains Porous," raised additional questions about the effect of the screener cutbacks on aviation security. The article also questioned whether TSA would be able to meet its extended deadline for scanning all baggage for explosives by machine by December 31, 2003.

- The article stated that not all of the machines purchased by TSA to scan checked luggage for explosives are being used.

  a) How many explosives detection machines currently installed in airports are not being used to their full capacity?

Answer: The exact number varies, as do the reasons why the equipment is not utilized to its full available capacity. Estimates indicate, however, less than 5% of the baggage screening equipment installed nationwide is being utilized at substantially less than full capacity. There are some airports, primarily in large high-volume metropolitan areas that have experienced chronic staffing difficulties. However, there are a variety of other circumstances that result in less than full utilization of the available capacity of installed equipment, peaks in airline schedules, and temporary maintenance and repairs.

b) Have the reductions in the screener workforce led to reductions in the usage of these machines?

Answer: Several of the airports using non-electronic screening methods are doing so due to screener workforce shortages. The majority are utilizing non-electronic screening methods include those that require extensive work to install in-line EDS solutions. Other airports in this category were experiencing short-term equipment outages that were resolved quickly or which had unusually high passenger volumes during peak travel times.

c) What steps has TSA taken, and what additional steps if any will TSA take, to ensure that it has adequate numbers of trained screeners to staff these machines at full capacity?

Answer: Since June 2003, TSA has focused its staffing efforts on airports that have a critical need for baggage screeners. Although staffing issues remain at a number of airports, the recruitment mitigation strategy has helped TSA maintain staffing levels required to operate baggage screening equipment. Additionally, TSA has formulated a FY04 supplemental budget request that will allow a more appropriate level of staffing for both baggage and passenger security screening.

d) If there are other reasons these machines are not being used, or used to full capacity, please explain.

Answer: There are several additional reasons why equipment may not be utilized to full available capacity. One frequent circumstance is that screening equipment was initially installed in more labor intensive and less efficient configurations, for example manually loaded lobby installations of EDS equipment, in order to meet the December 2002 deadline for 100% checked baggage screening. We are now re-evaluating and fine tuning many of these installations by relocating, reconfiguring or replacing equipment with more efficient configurations and equipment. Another reason has been equipment maintenance and repair problems. Following the installation of massive amounts of new equipment, we have experienced not only the normal warranty period failure that are to be

expected, but in some cases we have had to swap out equipment for different devices more suitable to the individual airport applications. These problems are progressively being remedied and the necessary adjustments being made as we normalize the operations of the massive equipment infrastructure that we have put in place.

- Section 425 of the Homeland Security Act directed TSA to report to Congress with a detailed plan on the deployment of explosives detection machines in airports that did not meet the original 2002 deadline, and to also submit interim reports on its progress in meeting this goal.

  a) Have these plans and reports been submitted on schedule? If not, why not?

     Answer: Since 12/31/02, TSA has submitted monthly reports to Congress providing the status of its efforts to deploy and install explosive detection technology

  b) When will plans for installing explosives detection machines in all airports be completed?

     Answer: TSA continues to work with the airport authorities at those airports where additional equipment is needed. The efforts are ongoing and must allow for flexibility based on changed conditions that can occur at any airport, for example, new air carrier start-ups, movements of air carries between terminals, construction of new terminals and increasing passenger loads. Additionally, many airports are seeking in-line screening solutions to allow for the removal of explosives detection equipment from the public lobby areas to the baggage make-up areas within the restricted areas of the airport.

  c) When will all of the required machines be installed and operational?

     Answer: TSA will be able to electronically screen all checked baggage at all airports by 9/30/04. However, that will not be the completion of TSA's efforts to install explosives detection technology. Efforts associated with in-line baggage screening solutions will be ongoing. Construction and facility modifications necessary to accommodate in-line solutions are expected to take several years to complete.

  d) Will there be any airports that have not completed installation of these machines by the end of 2003?

     Answer: Yes, there will be a few remaining airports where TSA will not be able to complete installation of sufficient numbers of explosive detection equipment needed to screen all checked baggage.

e) If so, when will all airports meet the requirement to have these machines installed and scanning baggage, including having sufficient screeners to operate these machines?

Answer: As previously stated, TSA will be able to electronically screen all checked baggage at all airports by 9/30/04. However, that will not be the completion of TSA's efforts to install explosives detection technology. Efforts associated with in-line baggage screening solutions will be ongoing. Construction and facility modifications necessary to accommodate in-line solutions are expected to take several years to complete.

FAMS and BICE

15. When authority for the Federal Air Marshal Service (FAMS) was transferred after September 11, 2001 from the Federal Aviation Administration to TSA, its size and mission were also dramatically expanded. As the Service began hiring and deploying new air marshals, a number of operational and control concerns emerged, including low morale, high turnover, lack of training, and scheduling inconsistencies. The Federal Air Marshal Service authority is now being transferred to the Bureau of Immigration and Customs Enforcement (BICE). What steps is DHS taking to ensure that challenges such as implementation of policies and procedures, communication across the agency, and the provision of information for management monitoring and oversight are effectively, clearly and fully addressed so that problems encountered during the previous transfer of FAMs to TSA are not experienced again during the transfer to BICE?

Answer: Operational and control concerns that were raised during the Federal Air Marshal Service stand-up phase have been fully reviewed by both the Department of Transportation's Inspector General, and the General Accounting Office. Each concluded that such concerns were either unfounded, or had been adequately addressed within the FAM Service.

Placement of the FAMS within the U.S. Immigration and Customs Enforcement (ICE) will strengthen the ability of the Department to coordinate its law enforcement activities by ensuring that all BTS law enforcement personnel are housed within the same agency. In addition, it will provide enhanced career path opportunities for ICE Agents and FAMs.

The missions of the FAMS and ICE are complimentary and compatible, and senior officials from the FAMS, ICE, TSA, BTS and DHS have been active participants in a number of transition working groups intended specifically to harmonize existing policies and procedures, develop new operational, managerial and communications procedures and strategies, and develop specific agreements to govern how basic administration functions will be handled during and after the transition period. We do not anticipate that there will be any obstacles to seamless implementation of policy, communication, management or programmatic oversight across the agency.

Interoperability

16. At present fire, police, EMS, and other public safety personnel cannot effectively communicate due to a lack of interoperable systems. This is not only a problem during major incidents involving large numbers of local, state, and federal agencies – but is an issue that impacts first responders daily in local communities. As long as first responders cannot communicate with one another, their lives, and the lives of the public, remain at greater risk. Project Safecom, which is now housed in the Science and Technology Directorate of the Department, serves as an umbrella programs within the federal government to coordinate the efforts of local, tribal, state and federal public safety agencies working to address this problem. With 44,000 different public safety organizations in the country, and an estimated cost of at least $18 billion in order to modernize our communications systems, resolving this problem will require sustained leadership, as well as resources, from DHS.

- As Deputy Secretary, what role would you play in addressing this issue?

  Answer: The Federal government has an important role in helping public safety agencies at all levels achieve communications and interoperability goals. As the Deputy Secretary of Homeland Security, I intend to support the Department's mission to provide focused and sustained leadership from the Federal government to the nation's public safety community. Over 90 percent of the public safety infrastructure is owned and operated at the local and State level. I believe that that the Federal government must work as a full partner with local and State first responder agencies to help those agencies achieve interoperability with each other, and to help the Federal government achieve interoperability with them.

  Working through the Directorate of Science and Technology (S&T), I will support the SAFECOM Program Office in its leadership role in addressing the issues of public safety communications and interoperability. As a public safety practitioner-driven program, SAFECOM is working with existing Federal communications initiatives and key public safety stakeholders to address the need to develop better technologies and processes for the cross-jurisdictional and cross-disciplinary coordination of existing systems and future networks. I support SAFECOM's role in promoting the development of new technologies, improved processes, and assistance to local, tribal, State and other federal agencies. SAFECOM will work with the entire public safety community in the planning, implementation, and operation of interoperable communications systems through outreach efforts to communicate best practices, coordinated funding guidance, and technical assistance.

- Do you believe that it should be at the top of DHS's list of priorities for supporting first responders and, if so, when can the American people expect that this problem will be fully resolved?

  Answer: The Department of Homeland Security is acutely aware of the need to promote public safety communications and interoperability. DHS understands

that inadequate and unreliable wireless communications have been issues plaguing public safety organizations for decades. In many cases, agencies cannot perform their mission critical duties. These agencies are frequently unable to share critical voice or data information via radio with other jurisdictions in day-to-day operations and emergency response to incidents including acts of terrorism and natural disasters, and are hence unprepared to protect the lives and property of this Nation in emergencies. That is why DHS accepted responsibility for SAFECOM, the President's initiative to find a solution to public safety interoperability shortfalls.

DHS also understands that the Nation is heavily invested in an existing infrastructure that is largely incompatible. As the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets observes, "most systems supporting emergency response personnel have been specifically developed and implemented with respect to the unique needs of each agency." Such specification without regard to the need for interoperability complicates the ability of agencies to effectively communicate with others in the future. Currently, agencies are often equipped with incompatible and aging communications equipment, are struggling to improve existing systems within limited and fragmented budget cycles and funding, have limited and fragmented planning and coordination between agencies, must work with a limited and fragmented radio spectrum, and have limited equipment standards available for their use.

The solution to the problems of public safety communications and communications interoperability—short of a major overhaul of how spectrum is allocated and managed in this country—is not a single, nor even a particular set, of discrete tasks. In other words, there are no simple solutions. Instead, the identification and orchestration of many programs is required. DHS, through SAFECOM, is employing a systematic approach to address these issues, inclusive of the following components:

- Identification of the problem, recognizing that it is a simple problem with many complex elements and no single solution.
- Collaboration with the leadership of the public safety community to gather comprehensive communications requirements in order to develop appropriate approaches to solutions, referred to as work packages. (This is essential since 90 percent of the public safety infrastructure is owned by State and/or local public safety entities.)
- Identification of current initiatives addressing interoperable communications issues and development of a coordination strategy to leverage existing work, while decreasing unnecessary duplication of efforts.
- Implementation of a strategy to develop short- and long-term projects to address public safety communications and communications interoperability requirements.

In partnership with the public safety community, SAFECOM is promoting interim solutions that will provide basic interoperability within one to three years. SAFECOM has also begun to promote more advanced, enhanced communications technologies and processes that will be achievable in the five to ten year time frame, followed by an eventual goal of ubiquitous communications in twenty years. This is an aggressive time line when we take into account the needs of 44,000 diverse public safety agencies.

- What is the current level of resources, in terms of staff and expertise devoted to Project Safecom? How can you be sure that it is sufficient?

  Answer: Several government programs have accomplished much in addressing the issues associated with public safety communications and interoperability. Unfortunately, much of this work has been disconnected, fragmented, and often conflicting. In an effort to coordinate the various federal initiatives, SAFECOM was established by the Office of Management and Budget (OMB) and approved by the President's Management Council (PMC) as an electronic government (E-gov) initiative to address public safety communications issues. SAFECOM is now firmly established in S&T and is beginning to ramp up its resources, both in terms of funding and staff.

  SAFECOM has successfully leveraged the knowledge and expertise of existing programs such as the National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards (OLES) and the Department of Justice's AGILE Program. These partnerships, coupled with the close relationship to other federal programs and to the national associations representing the leadership of the public safety and first responder communities, have allowed SAFECOM to hit the ground running as it develops research portfolios, test and evaluation programs, pilot projects, technology assistance efforts, coordinated grant guidance, and standards initiatives.

  SAFECOM is currently staffed by Federal employees and contractors. The Director and a chief of staff are now onboard, and recruiting is underway for four more Federal positions. Contract staff provides various forms of support, ranging from program management activities to outreach and technical support.

Emergency Response Funding

17. In July, an independent Task Force sponsored by the Council on Foreign Relations issued a report, which found that our nation remains "dangerously ill-prepared to handle a catastrophic attack on American soil." The report was compiled by a distinguished group of citizens, and was chaired by former Senator Warren Rudman. Much of the data the Task Force collected regarding our emergency response needs came from professional associations that provided information directly from the emergency responder communities they represent. They found that on average, fire departments across the country have only enough radios to equip half the firefighters on a shift, and breathing apparatuses for only one third. Only ten percent of fire

departments in the United States have the personnel and equipment to respond to a building collapse. Police departments do not have protective gear to safely secure a site following an attack with weapons of mass destruction. Public health labs in most states still lack basic equipment and expertise to adequately respond to a chemical or biological attack. In all, the report found that at current funding levels, America would fall approximately $98.4 billion short of meeting critical emergency responder needs over five years. Yet, DHS has consistently maintained that current funding levels are sufficient.

- If you were confirmed as Deputy Secretary, what would you do to clarify the disparity between what DHS currently maintains about the necessary funding levels and those of the Task Force of the Council on Foreign Relations?

- What would you recommend that DHS do to conduct its own thorough assessment of our nation's emergency response needs?

Answer: ODP established the State Homeland Security Assessment and Strategy (SHSAS) Process in fiscal year 1999 to assess, both at the state and local levels, threats, vulnerabilities, capabilities and needs regarding weapons of mass destruction terrorism incidents. This process has and continues to assist ODP and its partners in allocating federal resources for homeland security, and to serve as a planning tool for state and local jurisdictions. This year through ODP, DHS refined the SHSAS process to address a broader definition of homeland security. ODP worked closely with state, local and federal partners including FEMA, CDC, USDA, EPA and the FBI. The SHSAS process is the only process of its kind to comprehensively assess the homeland security needs of state and local agencies, therefore the Department intends to work with its partners to continue to further refine the process.

DHS, through ODP, currently conducts assessments of the nation's emergency response needs, both at the state and local levels, through the State Homeland Security Assessment and Strategy (SHSAS) Process. This process requires that each state and jurisdiction identify its planning, organizational, equipment, training, exercise and technical assistance needs. This process not only provides states invaluable information on how best to spend their homeland security funds, but it provides DHS information on national-level needs and vulnerabilities.

Funding to Local Governments

18. Mayors across the country have consistently complained that homeland security funds to protect the American people are not getting to the front lines with sufficient dispatch. The United States Conference of Mayors underscored this fact most recently in a September 2003 survey of 168 cities in all 50 states. The survey was designed to document the extent to which federal homeland security funding is actually reaching the nation's cities. The Conference asked cities about ten different homeland security funding programs for which applications had been solicited from states and a few other entities by the federal government through late July. It found that as of August 1, 90 percent of the survey cities had not received any of the $1.5 billion in funding for first responders and critical infrastructure protection. Thirty-seven percent of the

cities had been notified that funds would be received, but 53 percent had neither received funds nor been notified that they would. If you were confirmed as Deputy Secretary, what would you do to ensure that funding gets to the local communities where it is needed most as quickly as possible?

Answer: The Department of Homeland Security is committed to providing resources and assistance to states and localities in the most efficient and effective manner possible. The Department recognizes that in order for state and local jurisdictions and first responders to be effective partners with the federal government in securing our homeland, they need quick and easy access to the terrorism and emergency preparedness grant programs designed to support their work.

We at DHS are convinced that these programs must be more centralized and more accessible. It is our goal to provide state and local authorities a single point of contact for terrorism and emergency preparedness efforts – one access point to obtain critical grant funding. The Department's recent announcement of a "one-stop-shop" application for three different programs administered by the Office for Domestic Preparedness is an important step in this direction. The single application allows states to apply online for their allocated grants that benefit first responders and will provide additional resources to state and local government counterterrorism efforts.

This consolidation was done to streamline the grant application process and better coordinate federal, State and local grant funding distribution and operations. The homeland security assessments and strategies currently being finalized by the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, U.S. territories, and selected urban areas for submission to DHS-ODP will play a pivotal role in the identification, prioritization, and allocation of financial resources provided through the three grant programs. The funding provided will be applied against critical resource gaps identified through the assessments and prioritized in the State strategies.

Providing funds through a single application and award process facilitates coordination of preparedness activities related to the goals and objectives identified in the State strategies, resulting in a more effective and efficient use of funding. A single application also minimizes time spent on the application process and consolidates reporting requirements.

Additionally, the FY 2004 Department of Homeland Security Appropriations Act includes language that requires that ODP make formula-based funds available to the states within 30 days after enactment of the appropriations act. It also requires states to apply for their allocated funds within 30 days of the grant announcement and requires ODP to act within 15 days after receipt of an application or receipt of the updated state homeland security strategy, which is a requirement for states receiving their formula-based grant funds. The FY 2004 appropriations act also requires that each states obligate no less than 80 percent of the total award to local governments within 60 days after the grant is awarded.

In addition, ODP made application packages for the Fiscal Year 2004 Homeland Security Grant Program (which includes the State Homeland Security Grant Program, the Law Enforcement Terrorism Prevention Program, and Citizen Corps Program) available to the states on October 31, 2003, which was 30 days after the FY 2004 Department of Homeland Security Appropriations Act became law. Further, ODP made application packages for the FY 2004 Urban Areas Security Initiative available on November 12, 2003, which was 46 days after the FY 2004 Department of Homeland Security Appropriations Act became law.

Catastrophic Planning

19. Two recent emergencies, the blackout in the northeast and Hurricane Isabel, dramatically demonstrated vulnerabilities to our critical infrastructure and raise serious questions about our preparedness to respond to far worse natural disasters or a catastrophic terrorist attack. I am especially concerned that the Department of Homeland Security has not adequately assessed the specific shortcomings of our power and water infrastructure, much less implemented protective measures, and developed the kind of catastrophic emergency response plans necessary to ensure vital services are available following a major disaster or catastrophic terrorist attack. I also understand that there are concerns among some professionals within the emergency management community that our existing policies, plans, procedures and resources are not adequate to cope with the aftermaths of a truly extraordinary disaster.

- If you were confirmed as Deputy Secretary, what role would you play in ensuring that we have adequate plans in place for providing food, shelter, medical care, and water for hundreds of thousands or even millions of citizens in the aftermath of a catastrophe?

- What is the extent of the Department's current efforts to plan for a catastrophic or cataclysmic event in which, among other things, power and water would be disrupted for indefinite periods of time perhaps leaving millions of citizens without vital services? Who is involved and how much time and resources are being devoted to this effort?

Answer: Catastrophic planning is one of the Department and FEMA's top priorities. DHS believes that catastrophic planning is an essential component to ensure our national security and long-term economic interests. On a more fundamental level, catastrophic planning serves as a vital foundation to save lives and protect property--; and will ensure an effective long-term recovery process.

The DHS Emergency Preparedness and Response Directorate, FEMA provides leadership for catastrophic planning by working with Federal department and Agencies to ensure an effective level of federal preparedness and assists State and local emergency management and response organizations with appropriate planning. These efforts compliment the Department' s other programs to, train, equip and exercises our "first responders." Together they work to build and sustain the capability to respond to any type of catastrophic event.

In addition, FEMA maintains the operational capability to execute integrated response and recovery operations and programs in anticipation of and following Presidentially-declared disasters and emergencies, under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288, as amended.

Public Law 108-90, the Department of Homeland Security Appropriations Act, 2004, provided $180 million for Fiscal Year (FY) 2004 Emergency Management Performance Grants (EMPGs). EMPG funds assist local governments in developing comprehensive plans, linked through mutual aid agreements, outlining the specific roles for all first responders (fire service, law enforcement, emergency medical service, public works, etc.) in responding to terrorist incidents and other disasters. DHS is strongly encouraging States to use a portion of their Fiscal Year 04 EMPG funding for catastrophic planning.

In addition to FEMA's leadership in catastrophic disaster planning, the Department of Homeland Security is establishing a single, comprehensive national incident management system, as called for in Homeland Security Presidential Directive 5 (HSPD-5), Management of Domestic Incidents.

The National Incident Management System (NIMS) will provide a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from all domestic incidents, regardless of cause, size, or complexity.

To provide for interoperability and compatibility among Federal, State, and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies. HSPD-5 identifies these as the incident command system; multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources.

Mutual aid is a top priority for FEMA and the Agency is working to establish a comprehensive, integrated National Mutual Aid and Resource Management System to ensure an efficient and effective response to all hazards in support of NIMS. Under this system, federal, state, and local government agencies may request and receive resources quickly and effectively. Senior officials and elected leaders at all levels of government will have a snapshot of a real-time inventory of federal, state, and local response assets that are available through mutual aid, their operational status, and the conditions that need to be met to acquire them. The initiative supports the NIMS by establishing a comprehensive national mutual aid and resource management system that provides the basis to type, inventory, order and track all (Federal, State and local) response assets.

This resource management system will hold a national inventory of response assets, and serve as a tool to request, order, and track resources at all levels of government. The system will provide emergency managers with an accurate perspective of the national response capability, including federal, state, and local resources. It will not be a federal system that supplants state or local efforts, rather a system that will meet the needs of states and locals responding to small disasters as well serve a national response to large or catastrophic disaster.

Information Sharing

20. America's safety demands that state and local officials, especially law enforcement and public safety professionals—our front line defenders—are fully engaged in the war against terrorism. Yet, a recent report by Governmental Affairs Committee (GAC) Minority staff found that these officials are being asked to fight the war against terrorism with incomplete and unreliable access to one of the most potent weapons in the homeland security arsenal: information. State and local first responders and first preventers still do not systematically receive the information they need to prevent or respond to another catastrophic terrorist attack, nor does vital information flow effectively from them to the federal government. These information gaps pose a significant challenge for the federal government and leaves the American people at unacceptable risk.

- If you were confirmed as Deputy Secretary, what management steps would you implement to ensure that information sharing with state and local officials is a top priority for DHS managers?

  Answer: Information sharing with state and local officials is already a top priority for DHS managers. In particular, both our Office of State and Local Government Coordination and the IAIP directorate are focused primarily on finding ways to improve information sharing. I will, of course, ensure that continued attention and focus is put on this issue.

- Would you link success at effectively identifying and overcoming barriers to sharing appropriate homeland security information with bonuses for key officials?

  Answer: It is a reasonable proposal to link success at effectively identifying and overcoming barriers to sharing appropriate homeland security information with bonuses for key officials. The department certainly will take this under consideration in the future.

- How do you propose ensuring that state and local officials have a seat at the table to ensure that their homeland security information needs are met by DHS and other federal agencies?

  Answer: The good news is that State and local homeland security officials already have a seat at the table, and are both providers and recipients of homeland security information. For example, the homeland security advisory council has a State and local working group, which facilitates communication among states and localities on homeland security issues. In addition, we regularly form ad hoc State and local advisory groups to assist in the development and implementation of Homeland Security policies. Finally, the Office of State and Local Government Coordination regularly consults with State and local officials as well as the major associations that represent them. Feedback from out State and local constituency indicates that these improvements are making a difference.

Science and Technology

21. How much do you expect HSARPA will spend and obligate in FY 2004? How much did it spend and obligate in FY 2003? Please break down these expenditures by describing funding amounts spent in particular issue areas (for example, biological threats, chemical threats, port security IT, etc.). Please describe the types of organizations and agencies HSARPA R&D grants, by total amounts, are going to, such as universities, industry, NIH, Defense, etc. How many employees does HSARPA now have and how many more is it expected to employ by the end of FY 2004?

Answer: The Science and Technology Directorate (S&T) is currently in the process of evaluating FY2004 proposals and determining the HSARPA allocation for FY2004.

In FY2003, HSARPA was just being stood-up. The Director reported for duty on September 2, 2003. As a result, there were no substantial obligations or expenditures in FY2003. The S&T program was executed by the Directorate as a whole. However, one project was specifically started in FY2003 by HSARPA in collaboration with the United States Coast Guard (USCG). The prototype integrated maritime surveillance system testbed effort in the South Florida region started in August FY2003 ($2.361M in FY2003). The $4.0 million, 24-month program will integrate existing facilities and upgrade equipment to detect, track, and identify vessel traffic around ports, in the zones around ports, and over the horizon. This evolutionary testbed will provide an immediate coastal surveillance capability in a high priority area. In the future, it will offer the USCG and

other Departmental organizations the means to develop operational concepts, and implement and test interoperability between Homeland Security and Department of Defense systems and networks. Project planning included the USCG FY2004 Research, Development, Test and Evaluation (RDT&E) appropriation funding of $300K for an operational and technical evaluation of the project.

HSARPA has a solicitation extant for Detection Systems for Biological and Chemical Systems Countermeasures. There are 518 responses now under evaluation. HSARPA expects to enter contract negotiations with the selected proposers in January 2004.

HSARPA issued its first Small Business Innovation Research (SBIR) Program Solicitation on Friday, 14 November 2003. The solicitation invites small businesses to submit innovative research proposals that address eight high priority DHS requirements: new system/technologies to detect low vapor pressure chemicals; chem-bio sensors employing novel receptor scaffolds; advanced low cost aerosol collectors for surveillance sensors and personal monitoring; automated vulnerability assessment of u.s. infrastructure; marine asset tag tracking system; AIS tracking and collision avoidance equipment for small boats; ship compartment inspection device; advanced secure supervisory control and data acquisition (SCADA) and related distributed control systems. The planned FY2004 SBIR budget for two Phase I rounds and one Phase II round is the required 2.5% of the RDT&E extramural budget.

HSARPA expects to issue at least three more solicitations for industry and academia in FY2004 on topics such as: radiological and nuclear countermeasures, conventional explosives detection, and cybersecurity.

HSARPA has not issued any R&D grants to date. Our biological/chemical systems solicitation expects to award "Other Transactions for Research and Prototypes" contracts to meritorious proposers who are primarily from industry and academia.

The first HSARPA employee, Dr Jane Alexander, Deputy Director, became a DHS employee on August 10, 2003. The current HSARPA staff of nine includes Dr David F. Bolka, HSARPA Director, and seven full time employees. They are supported (*pro tem*) by 20 support contractors.

The HSARPA staffing plan calls for a total of 62 full time employees comprised of 30 full time technical program officers and leaders, with 32 support staff. HSARPA expects to be almost fully staffed by the end of FY04.

22. When will the Science and Technology Directorate have both initially stood up and placed into full operation the Homeland Security Institute? How many employees will the Institute employ when at full strength, and when is it expected to reach this level? Will the Institute focus on the risk and threat analysis tasks assigned by Congress? If not, why not? If so,

what particular risk and threat analytical work will it support? What other R&D tasks will it undertake?

Answer: The Science and Technology Directorate is actively working to implement the Homeland Security Institute in accordance with the requirements of the Homeland Security Act of 2002 (Public Law 107-296).

The S&T Directorate, working through the United States Army Medical Research Acquisition Activity (USAMRAA), plans to release a formal solicitation for proposals in December 2003 to create the Homeland Security Institute. Proposals will be received in February 2004, with an initial award scheduled for July 2004. At full strength, the Institute will employ approximately 150-200 people, reaching this level in 2005.

The Institute will provide dedicated, sole-source, high-quality technical and analytical support capabilities to inform homeland security decision making across all areas of the Department's responsibilities. The Institute's studies and analyses will address all tasks (e.g., risk and threat analysis) identified in Sec. 312. of the Homeland Security Act of 2002.

Core competencies will be created in four areas: (a) systems evaluations, (b) technology assessments, (c) operational assessments, and (d) resource and support analyses.

- Systems evaluations will provide analyses that will support homeland security program planning and execution. Analyses will cover all stages of development: initiation/conduct of research; development of technology; testing, evaluation, building/acquiring, deploying and using systems. The Institute's analysis work will use systems analysis, risk analysis, and simulation and modeling to determine: (a) vulnerabilities of the Nation's critical infrastructure, and (b) effectiveness of systems deployed to reduce those vulnerabilities, including potential threats and countermeasures to systems.
- Technology assessments will provide scientific, technical, and analytical support for the identification, evaluation, and use of advanced technologies for homeland security systems.
- Operational assessments will be conducted that relate systems development, operational performance, and homeland security strategy; these assessments will lead to both revised operational concepts and mission needs.
- Resource and support analyses will develop methods, techniques, and tools, and conduct analyses that will lead to improved means for addressing resource issues including investment decisions and cost implications of pending decisions.

23. What relationships, by contract or other agreement, with existing federally funded research and development centers (FFRDC's) have the Science and Technology Directorate and the Department entered into? Please briefly describe each such relationship including the type of R&D work to be pursued. What additional new FFRDC's is the Directorate contemplating and in what areas of R&D work? Please describe the R&D work the Directorate has commissioned

at Energy Department research and laboratory facilities, including FFRDC's, and the level of Departmental expenditures at such facilities.

Answer: The Science and Technology (S&T) Directorate's current relationships with Federally Funded Research and Development Centers (FFRDC's) are mostly with Department of Energy (DOE) national laboratories. The Science and Technology Directorate has also issued a Task Order under a Department of Defense (DOD) contract to another FFRDC, which is identified in subsequent text. In addition, S&T, working through a Task Order in place through DHS/BCIS/BCP, contracted with MITRE Corp., an FFRDC, to provide systems engineering support for U.S. VISIT program. The S&T Directorate also recently placed a contract with Lincoln Labs, another FFRDC, through HSARPA. We are also considering the possible designation of one new FFRDC in addition to the Homeland Security Institute discussed in Question 22 above.

The Science and Technology Directorate conducts portions of its intramural programs at DOE national laboratories as provided for in sections 308 and 309 of the Homeland Security Act of 2002. Several DOE national laboratories that are also FFRDCs participate in S&T programs. These FFRDCs include the Argonne National Laboratory, the Brookhaven National Laboratory, the Idaho National Engineering and Environmental Laboratory, the Los Alamos National Laboratory, the E.O. Lawrence Berkeley National Laboratory, the Lawrence Livermore National Laboratory, the Oak Ridge National Laboratory, the Pacific Northwest National Laboratory, the Sandia National Laboratories, and the Savannah River Technology Center. In addition to the work at these FFRDCs, S&T also has work underway at the Remote Sensing Laboratory, operated by the Bechtel-Nevada Company and providing access to DOE's Nevada Test Site.

The programs underway at the DOE facilities are typically multi-disciplinary research and development programs across several S&T technical portfolios. These portfolios include Biological Countermeasures; Border and Transportation Security; Emergency Preparedness and Response; Threat and Vulnerability, Testing and Analysis; Radiological/Nuclear Countermeasures; and Development of Standards. In addition, S&T has obtained personnel from DOE and its site and laboratory contractors to assist in the technical management of the Directorate's portfolios. In Fiscal Year 2003 S&T committed $126M to the DOE facilities. To date in FY2004, a further $13M has been committed and we expect this year's total to approach $150M - $200M.

The Science and Technology Directorate has issued a Task Order under the DOD contract sponsoring the Institute for Defense Analyses (IDA), a DOD FFRDC. IDA will be the lead contractor for managing the implementation of the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) established in section 861 of the Homeland Security Act of 2002. IDA's work will include development of evaluation criteria and identification of expert review panelists for evaluating SAFETY Act proposals.

Under section 305 of the Homeland Security Act of 2002, the Secretary, acting through the Undersecretary of S&T, has the authority to establish a FFRDC. At this time S&T

has begun to study the issues and benefits that would be associated with establishing an FFRDC at the National Biodefense Analysis and Countermeasures Center (NBACC) at Ft. Detrick, MD. At this time S&T has not completed its analysis but expects to do so during FY2004

24. How many professional employees at the S&T Directorate come from the Department of Energy and its laboratory system compared to the Directorate's total professional employee base? Of these, how many have continuing employment or other ties to DOE or its labs?

Answer: The Science and Technology Directorate is authorized a total of 180 FTEs in FY2004 plus the 61 authorized FTEs of the Environmental Measurements Laboratory (EML) which was transferred to the Department of Homeland Security (DHS) by the Department of Energy (DOE) in FY2003. A total of 53 existing EML personnel were transferred from DOE to DHS S&T in FY2003; an additional 6 FTEs were transferred from DOE to DHS with the transfer of programmatic responsibility and funding via Determination Order in FY2003.

The S&T Directorate had a staffing level, including EML, of 217 effective October 20, 2003, of which 185 are professional staff. Included in the professional staff are 5 DOE Headquarters staff plus 41 DOE EML staff who transferred from DOE to S&T via Determination Order in FY2003. An additional 2 professional staff are on detail to S&T from DOE and 2 professional staff from DOE were hired by S&T. A total of 23 professional staff from DOE National Laboratories are on assignment to S&T through the Intergovernmental Personnel Act or contract. This information does not include staff working on S&T funded projects at the DOE laboratories.

AFFIDAVIT

I, James M. Loy being duly sworn, hereby state that I have read and signed the foregoing Statement on Pre-hearing Questions and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

Subscribed and sworn before me this 17th day of November, 2003.

Notary Public

Questions from Senator Lautenberg

1. **Why are Principal Security Inspectors allowing for home study courses of important security procedures as part of air carrier training programs for flight attendant security? Do you feel this is an adequate substitute for hands-on training? Does this "home study" approach present a risk of providing a roadmap for terrorists should they get ahold of this home study material? What do you feel is appropriate for protecting this information from the public domain?**

   Answer: As of today, there is no regulation or requirement that would preclude flight attendants from receiving security training at home. Prior to 9/11/01 FAA regulations required that all air carrier training programs be developed by air carriers and approved by FAA -- a job delegated to Principal Security Inspectors. In the aftermath of 9/11 two new laws changed flight attendant training requirements and a third is awaiting passage by the Senate. The first change provided updated guidance to air carriers and the air carriers had to change their training accordingly and again submit it to FAA for approval -- again with the PSI's in the role of approving official.

   The second law, the Arming Pilots Against Terrorism Act, required TSA to issue a regulation to implement yet another enhanced training program. As of this time, TSA has not issued the rule and has yet to finalize how the APATA training requirements will be developed, reviewed and approved. The current situation is further complicated because of the pending passage of the FAA Reauthorization Act which, when enacted would change the APATA requirements. So what is in effect right now are the requirements of the first law passed after 9/11 which is the Aviation Transportation Security Act under which PSI's are the approving officials for the flight attendant training.

   Hands-on training has demonstrated value as a training method. However, since the hands-on training components of the curriculum contemplated by APATA are not fully developed, it is difficult to precisely assess how much added value it would bring.

   All training materials are classified as Sensitive Security Information and the obligation of the individual who possesses it does not change whether it is in a classroom or at home. There are requirements to protect SSI information, not to disseminate and not to disclose it publicly. I do not agree that SSI training materials presented in the classroom setting are necessarily more secure that those same materials used at home.

2. **Do you feel that the Department, through the Transportation Security Administration, is able to develop security training standards to adequately provide for cabin crew security aboard passenger aircraft while not financially overburdening air carriers?**

   Answer: Yes, the Department and TSA can develop a crew member self defense training program that will improve upon existing crew member training requirements, while giving full consideration to the impact on the airline costs and other factors. In fact,

under APATA, TSA is required to issue a rule, which, by its very nature, offers an opportunity for impacted persons and business to comment on the proposed rule. Air carriers, for example, would be able to offer information during the notice of proposed rulemaking on the rule's impact in terms of costs and other factors they believe have a bearing on what the rule might impose. All of these issues would be evaluated by TSA. Ultimately, any rule we would issue in this regard would ensure that the intent of the law was met and that it was done in a reasonable manner, accommodating all stakeholders as best as possible.

3. **With respect to the Coast Guard, how do you plan in your new post to oversee the development of both the vessel and facility security plans as well as the area maritime security plans for our nation's ports and port communities?**

   Answer: I met with Admiral Collins on November 10th and received a full briefing on the Coast Guard's plans to implement the various requirements of the MSTA. I am confident they are on target and tracking. For example at the local level, Coast Guard Captains of the Port have already established Area Maritime Security Committees, and these bodies will be instrumental to the development of the Area Maritime Security Plans by the June 1, 2004 approval deadline. Also, while the responsibility of developing domestic vessel and facility security plans reside with industry, the Coast Guard has a sound strategy to meet the aggressive July 1st approval deadline.

   I am also supportive of the Coast Guard's plan to verify the existence and implementation of security plans approved by the flag state for foreign vessels calling on the United States. During my tenure as Commandant, I stood before the International Maritime Organization and called for the development of an international scheme for port and shipping security, and our desired security requirements form the basis of the current International Ship and port Security (ISPS) Code that has been adopted by over 100 nations. By leveraging the partnership of these nations, we have a powerful force multiplier in improving maritime security. However, while we will trust flag states to adhere to their international obligations, we will use an aggressive port state control program to verify the international shipping community is effectively employing the ISPS standards in order to be allowed to conduct trade with the U.S.

4. **In the area of the Port of NY/NJ we have the Indian Point reactor located adjacent to navigable waterways. The Coast Guard has said that they don't plan on including Indian Point in the vessel and facility security plan because its not part of a transportation system and does not have the capability to dock incoming ships. But they have said that Indian Point will be covered in the area security plan. Because a ship can be used as a weapon, much like the planes were used on Sept. 11, why wouldn't Indian Point be included in the vessel and security plan?**

   Answer: Nuclear power plants, and other facilities that are adjacent to navigable waterways, will not be directly regulated under the MTSA. However, the unique hazards they pose will be considered during the Coast Guard Captain of the Port's development of

the Area Maritime Security Plan, which takes a holistic approach to vulnerabilities in the maritime transportation security system, including neighboring plants and facilities.

The Nuclear Regulatory Commission (NRC) is reviewing and analyzing numerous threat scenarios and threat vectors including surface and sub-surface attacks to the water intakes of nuclear power plants. Upon completion of their assessment of the Indian Point Energy Center, we anticipate their assessment will be shared with the local Captain of the Port in New York/New Jersey to ensure that protective strategies are developed and included in the Area Maritime Security Plan mandated by the MTSA in order to address waterborne attacks if they are a high risk to the facility.

The protection of the facility is the primary responsibility of the facility owner and operator. Any local, state and/or federal resources needed to augment the security of this facility will be included in the Area Maritime Security Plan.

5. **Do you feel we're undermining the security of the busiest container port on the east coast by diverting the port of NY/NJ's fastest Coast Guard ships to duty in Iraq?**

Answer: No, I do not believe the security of the Port of New York/New Jersey was degraded for several reasons. First, prior to deploying the forces requested by the combatant commander, the Coast Guard carefully weighed the risks to homeland security and to overseas military operations. Only two cutters from the NY/NJ area, the BAINBRIDGE ISLAND and ADAK, both 110-foot patrol boats homeported in Sandy Hook, were sent overseas. The BAINBRIDGE ISLAND returned in June and has resumed her normal operations in an around New England. To meet daily and emergent threats within the vicinity of New York harbor area, other assets, including cutters from up and down the Atlantic seaboard, and Maritime Safety and Security Team (MSST) detachments from as far away as Texas, were utilized.

Additionally, the Coast Guard has been developing additional capacity in the NY/NJ area. In September, a MSST was established in New York. This team, which consists of 104 people and six armed boats, is specifically designed for the port, waterways, and coastal security mission. While the capabilities of a MSST are somewhat different than a patrol boat, their specialization, speed, and numbers greatly improve the maritime security posture in the port area.

Finally, the Coast Guard has leveraged the support of DOD for the homeland security mission as a resource force multiplier. As part of an agreement with the Navy, the Coast Guard received tactical control of 11 Navy, 170-foot Cyclone class patrol boats. These PC-170s are larger and faster than the Coast Guard WPBs, and any of the 7 assigned to the LANTAREA Commander could be quickly dispatched to the NY/NJ area to increase security.

Post-Hearing Questions Submitted by Senator Susan M. Collins,
Chairman, Senate Committee on Governmental Affairs; and
Senator Joseph Lieberman, Ranking Member, Senate Committee on Governmental Affairs
for the Nomination of James M. Loy to be
Deputy Secretary of Homeland Security
Tuesday, November 18, 2003

Question 1: Today's *Airport Security Report* includes an article that raises concerns about the reliability and adequacy of the L-3 eXaminer 3DX-6000s used to scan passenger checked baggage for explosives. Please comment on this article, a copy of which is attached. Specifically, please state whether TSA or any airports have experienced problems of the nature described in this report with the L-3 system. If so, please describe and state what actions TSA is taking to address these problems.

Answer: The article in question refers to a report that was neither produced by technical experts within TSA nor was sanctioned by the agency. Although there are continuing operational challenges with both types of EDS machines, those challenges are not outside what is expected for the complexity of the machines and the variations in their operating environments. TSA has a robust process in place whereby any such challenges, once they are identified, are quickly addressed and solved with the vendors.

Question 2: In March 2003, the U.S. Office of Special Counsel (OSC) released the results of an investigation regarding a whistleblower complaint brought by Mr. Bogdan Dzakovic. The report reflected findings of a related investigation by the Office of the Inspector General at the Department of Transportation, which, according to an OSC press release dated March 18, 2003, "substantiates the crux of Mr. Dzakovic's allegation: that the [FAA] Red Team Program was grossly mismanaged and that the result was the creation of a substantial and specific danger to public safety." According to the press release, the OIG "did not substantiate Mr. Dzakovic's allegations of deliberate cover-up or suppression of Red Team results."

The Special Counsel also expressed concern about possible retaliation against Mr. Dzakovic regarding his job duties at TSA. According to the March OSC release, you wrote a letter indicating that Mr. Dzakovic had been given meaningful work. However, according to the OSC release, the Special Counsel observed that "although Admiral Loy's letter states that Mr. Dzakovic has been assigned to a new position that will make full use of his experience, Mr. Dzakovic continues to assert that his new assignment (like the one that preceded it) involves "make-work" and does not befit someone of his training and background." Mr. Dzakovic contacted the Committee today (November 19, 2003), and alleged that he still is being denied meaningful work commensurate with his experience or salary.

Please comment on the allegation of retaliation against Mr. Dzakovic, and indicate what you have done to ensure that neither he nor any other whistleblower within TSA is subject to retaliation.

Answer: The whistleblower retaliation claims asserted by Mr. Dzakovic were the subject of mediation sponsored by the Office of Special Counsel (OSC) held on June 5 and September 29, 2003. The parties reached an agreement in principle, signed by the parties, on September 29 that fully resolved all claims raised by Mr. Dzakovic. The parties are now finalizing the settlement agreement.

All employees of TSA, including screeners, are now covered under the Whistleblower Protection Act. TSA continues to ensure that its employees are not subject to retaliation and cooperates fully with OSC when allegations of retaliation are raised.

Air Safety Week's

Airport Security Report

Business • Regulation • Technology • Operations

November 19, 2003
Washington, D.C.

Vol. 10 No. 23
www.aviationtoday.com

L-3 Reliability Questioned In Boston Bag Screening System

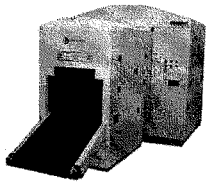
U.S. government-certified explosives detection systems (EDS) produced by **L-3 Communications** [NYSE: LLL] are experiencing significant operational problems at **Boston Logan International Airport** (BOS) that have gone unresolved for more than eight months and may cause the systems to be replaced, according to **Transportation Security Administration** (TSA) documents and sources interviewed by *Airport Security Report*.

The in-line screening problems are detailed in a document prepared in August by TSA personnel at Boston and obtained by *ASR*. The document compares the in-line bag screening systems at **San Francisco International Airport** (SFO), which uses **InVision Technologies** [Nasdaq: INVN] CTX-9000 EDS units, and Boston Logan, whose $146 million newly constructed baggage conveyor system depends upon 38 L-3 eXaminer 3DX-6000s to scan passenger checked baggage.

The document outlines operational deficiencies with the Boston in-line system's aperture, throughput, system availability, technical support and bag tracking when compared to InVision machines *(see comparison report, p. 2)*.

Nationwide, the TSA has spent more than $500 million on eXaminer 3DX-6000 acquisition and installation costs.

The most critical problem focuses on software glitches that cause the machine to produce incomplete X-ray images of passenger checked baggage. This function is of crucial importance, as Boston is designated the primary site to connect every L-3 machine to a dual-operator bag viewing station (BVS) whereby operators can examine suspect X-ray bag images produced by the EDS.



The eXaminer 3DX-6000 produced by **L-3 Communications** is the center of a controversy in the new in-line baggage screening system at **Boston Logan International Airport** (BOS). The machines experience software glitches that most critically result in incomplete X-ray images of passenger baggage, according to a TSA document.
Photo: L-3 Communications

In the dual-bag viewing station design, operators can clear a greater number of bags by viewing the X-ray image from a remote location, rather than performing a labor-intensive and time-consuming secondary explosives trace detection (ETD) exam or full hand search. But the incomplete images on some bags means more bags are defaulted to a trace examination and throughput is slowed.

The TSA document states **Massport**, Logan's airport authority, is paying $1.4 million annually in labor costs to overcome the L-3's small aperture. Directional devices are needed to guide bags into the machine because of a difference in widths between the conveyor belt and 3DX-6000. Massport has stationed personnel at the machines to prevent bag jams when bags are not lined up correctly. *Continued on page 4*

- **Comparison of Boston and San Francisco In-Line Screening Systems ..... Page 2**
- **Customer Base Prefers InVision ..... Page 4**
- **Australia's Virgin Blue Misses Hardened Cockpit Door Deadline ..... Page 6**
- **McCain: TSA Can't Gauge Screener Effectiveness ..... Page 7**
- ***ASR's* Breach Report ..... Page 8**

©2003 PBI Media, LLC. Federal copyright law prohibits unauthorized reproduction by any means and imposes fines of up to $100,000 for violations.

Comparison Of Inline Checked Baggage Systems At San Francisco And Boston

Measure of Effectiveness	Boston (L-3 Communications eXaminer 3DX-6000)	San Francisco (InVision Technologies CTX-9000)
APERTURE	• Restricted opening • Width 29.5 inches/Height 17 inches • Requires Directional Input Devices (DID) that lead to approximately 75 percent of all tracking issues • Massport currently spends $1.4 million annually in contract worker expenses to monitor the DID in order to prevent bag jams • Limited aperture resulted in the establishment of eight additional oversize/oddsize screening locations to facilitate the amount of checked baggage that cannot fit through the L-3 • Use of Explosives Trace Detectors (ETD) for screening of all oddsize/oversize bags not as effective as Explosives Detection Systems (EDS) screening	• Large opening • Width 39 inches/Height 41 inches • No DID required • No bag jams • Minimal tracking issues
THROUGHPUT	• Less than 300 bags per hour • 62 percent of advertised rate • 90 percent of total bag volume • Five bags per minute	• International Terminal – 360 bags per hour • Domestic Terminal – 450 bags per hour • 99 percent of total bag volume • Eight bags per minute
OPERATIONAL AVAILABILITY	• Less than 83 percent system availability • 10-15 minute reboot issue • No-image-in-buffer and incomplete images issues • Optimum performance requires dual-baggage viewing stations (BVS) • All operational issues are volume-dependant • Screeners must initiate resets which detract from overall security	• 98 percent system availability • Reboot requires less than 3 minutes • No buffer volume constraints • Screeners do not reset any EDS

To: PBI Media, LLC NC/RC
1201 Seven Locks Road, P.O. Box 61110
Potomac, MD U.S.A. 20854-1110
+1/301/354-2100 • 888/707-5812 • FAX: +1/301/309-3847
Telex: 358149 • E-mail: clientservices@pbimedia.com

Please ☐ enter ☐ renew the following subscriptions:
☐ **Airport Security Report**– 1 year for $797 (25 issues)
☐ **Air Safety Week** – 1 year for $1097 (48 issues)
☐ **Commuter/Regional Airline News** – 1 yr. for $897(48 issues)
☐ **Airline Financial News** – 1 year for $897 (48 issues)
☐ **Aircraft Value News** – 1 year for $997 (25 issues)

☐ MasterCard ☐VISA ☐AMEX ☐Discover

Card No._____ Exp. Date_____
Signature_____
Name_____
Title_____
Organization_____
Address_____
City _____ State_____ ZIP_____
E-mail Address: _____

Airport Security Report
ISSN 1078-1420

Editor: Eric Grasser
egrasser@pbimedia.com
Editorial Advisor: David Evans
devans@pbimedia.com
Managing Editor: Fred Donovan
fdonovan@pbimedia.com
Production Manager: Tracey Lilly

Director of Marketing: Jill Braun
jbraun@pbimedia.com
Publisher: Diane Schwartz
dschwartz@pbimedia.com
V.P. & Publisher: Heather Farley
hfarley@pbimedia.com
President & CEO: Don Pazour

For advertising, call:
Jill Braun, Director of Marketing
+1/301/354-1694, *jbraun@pbimedia.com*
Send press releases to:
Eric Grasser, Editor, +1/301/354-1823
FAX: +1/301/762-4196, egrasser@*pbimedia.com*

Subscription: $797 per year (outside North America add $49 for air mail; in CO, MD and TX, please add applicable sales tax). Reproduction of this newsletter in whole, or part, without prior written consent of PBI Media, LLC is prohibited. Federal copyright law prohibits unauthorized reproduction by any means and imposes fines up to $100,000 for violations. To order reprints contact Steve Mussman at 212-221-9595 x111 or email: reprints@parsinfl.com. For subscription information, see the attached coupon. Subscription and business offices: 1201 Seven Locks Road, Suite 300, Potomac, MD 20854. Phone: 301/354-2000.

Measure of Effectiveness	Boston (L-3 Communications eXaminer 3DX-6000)	San Francisco (InVision Technologies CTX-9000)
MULTI-PLEX CAPABILITY	• No such capability at this time • Documented communication problems with baggage handling systems • Needs mature communications infrastructure	• Demonstrated – solid performance • Communications infrastructure consists of robust Ethernet • Remote viewing stations at ETD locations
TECHNICAL SUPPORT	• Identified problems have gone unresolved for over eight months • Performance does not meet stated expectations • Insufficient number of repair technicians • No on-site integration expertise	• Outstanding technical support • From networked control room, technical personnel maintain operation • Provides both technical and integration expertise on-site • Aggressive system priority response
R&D (STRATEGIC APPROACH)	• Unaware of any current R&D efforts	• Past 18 months, InVision has spent $25 million of its own resources on improving its system
THREAT DETECTION	• Volumetric approach allows for 3-D reconstruction • No TSA performance standard/goal	• Slice approach is better at performing detection across finite cross-section • Better as an integrated component • No TSA performance standard/goal
SOFTWARE	• Software updates pending • Current software version has documented instability	• Continuous software upgrades
STAFFING	• Additional TSA staffing required to handle oddsize/oversize bags • Dual BVS screeners required • Airport Authority does not have dedicated baggage screening expert on payroll	• Multiplex capability reduces staffing requirements • Airport Authority has dedicated baggage screening expert on payroll that oversees all aspects of the in-line systems
FUTURE CONSTRUCTION	• Current Terminal A design needs to be adjusted to handle reduced L-3 throughput and aperture • Boston design team should approach TSA Headquarters concerning switching to CTX-9000s for Terminal A	• System designed with new technology (i.e. – X-ray diffraction) as a drop-in system component
FALSE-ALARM RATE	Comparable	
TRACKING	• Approximately 10 percent of all bags inputted into in-line system are mistracked • No recirculation capability	• Less than 2 percent of all bags are mistracked • Seamless recirculation capability requiring no manual effort
INTEGRATION	• Primarily contractor based; not well defined	• Dedicated program engineer
DECISION TIME	• Varies between 40 to 60 seconds • Bags constantly in motion • Incomplete image phenomenon	• Standard 80 seconds • If exceeded, automatically deferred to recirculation
TECHNICAL SUPPORT	• Parts availability • Consistent technicians/level of support • Limited offsite diagnostic ability • Unclear roles/responsibilities	• Networked control room • Robust preventative program
FUTURE ADAPTABILITY	• Currently limited	• System designed with this function (EDS can communicate with the Yxlon explosives detection system)

Source: Comparison prepared by Transportation Security Administration personnel at Boston Logan Airport

Continued on page 4

The TSA also has absorbed more funding costs since many oversize/oddsize check-in bags do not fit into the machine. Eight additional ETD stations have had to be positioned at Boston to screen those bags, compared to what would be needed with the InVision CTX-9000, the document states.

TSA officials at Boston suggest that InVision CTX-9000s be used in Logan's Terminal A, which is being rebuilt and is expected to reopen in 2005.

After L-3 became aware of the comparison document, Joseph Paresi, president of the firm's Security & Detection Systems Division, provided the document to TSA headquarters in Arlington, Va.

TSA's Randy Null, assistant administrator and chief technology officer, and John Shkor, associate administrator and chief operating officer, wrote Paresi on Aug. 29 in an effort to downplay the comparison.

"We would like to begin by assuring you that this is an unsanctioned effort by a non-technical TSA employee [at BOS], and does not reflect TSA's officially stated position on L-3's technology," Null and Shkor wrote in the letter obtained by *ASR*.

Had headquarters known of the document, the Boston personnel "would not have been authorized to release it," the TSA officials wrote. The officials said that rival firm InVision Technologies also would be informed that the "document in question is not an official TSA document, and therefore, cannot be used in any discussions with potential customers."

Shkor and Null apologized to Paresi "for any business difficulties that you may have encountered as a result of this document and authorize you to use this letter as a response to any customer inquiries you might receive regarding this document," the letter ended.

L-3 Communications and TSA would not comment on the BOS/SFO comparison.

TSA's Null told aviation security officials at an Oct. 21-22 industry safety and security meeting in Tampa, Fla., that stakeholders would rectify the L-3 software and customer service issues one way or the other, according to an airport security manager who attended the meeting and requested anonymity. But Null clearly sent the message "to get it fixed or it would be taken out," the source said. Replacing the L-3 equipment would be the least desired option to correct the system, as it would involve time and expense.

A source at San Francisco airport credited InVision for supplying excellent customer service in continuously improving its EDS software. The software improvements lowered false alarm rates and increased processing speeds, which were a big benefit in the international terminal for bothersome baggage going to Asia. Additionally, the airport has been able to process upwards of 450 bags per hour in the domestic terminal systems.

The airport may see throughput rates increase more in the future as it adds radio frequency identification (RFID) to the bag screening process. San Francisco also is a sight for multiplexing, InVision's networked version of the dual-BVS system used by L-3. When RFID is fully implemented, "certain bags that [set off the] alarm won't even be viewed by an operator, they'll just go straight to an [ETD or hand search] inspection," the source said.

L-3 System Problems Continue

While the report signals that the San Francisco system has worked well, none of the near dozen in-line systems at airports in the Unites States are perfect, and all of them are demanding and uncompromising.

L-3's problems with the eXaminer 3DX-6000 have been well documented since shortly after the machine was certified for EDS screening by the **Federal Aviation Administration** (FAA) in late 1998.

At a **U.S. Senate Aviation Subcommittee** hearing in April 2000, the **Department of Transportation**'s inspector general said that InVision's CTX-5500 model was the only FAA-certified bulk explosives detection device deployed at U.S. airports, although the L-3 unit had been certified for 18 months.

A month after the 9/11 terrorist attacks, DOT inspector general Kenneth M. Mead told the **U.S. House Aviation Subcommittee** that most of the nine L-3 EDS units purchased by the FAA were in a warehouse because air carriers refused to use them due to software and mechanical problems. In fact, one unit at **Dallas-Fort Worth International Airport** (DFW) leaked radiation. The machine experienced a mean time of 84 hours between failures requiring a maintenance service call, and a mean time to repair of almost six hours.

In an independent assessment of two machines at the FAA's tech center in New Jersey, the machines experienced high failure rates, mostly requiring software resets, Mead said. "The reliability issues need to be resolved before additional L-3 eXaminer 6000 machines can be deployed," he declared.

Steve Zaidman, FAA associate administrator for research and acquisitions, told House members in December 2001 that L-3 made some headway in correcting mechanical problems, but "not to the level we'd like to see, yet."

Is Politics To Blame?

The fact that only one other manufacturer passed U.S. certification testing may have influenced L-3s decision to not prioritize research and development costs to improve the eXaminer 3DX-6000, sources said.

Ironically, Congress is to blame for forcing the L-3 EDS unit into the marketplace at a time when the mechanical problems were prominent. L-3's production facility in Clearwater, Fla., is in the congressional district of the Rep. Bill Young (R-Fla.), chairman of the **U.S. House Appropriations Committee**.

Young's office entered language into the 2000 transportation budget that required the FAA to split $40 million between L3 and InVision and mandated a 1:1 purchase ratio, even though the mechanical and software problems were known. Included on L-3's lobbyist payroll was Linda Daschle, a former deputy FAA administrator and the wife of Senate Majority Leader Tom Daschle (D-S.D.).

Before 9/11, InVision dominated the EDS market in the United States with a 90 percent market share. Today, about 60 percent of the nearly 1,200 EDS units deployed across the country are InVision products.

InVision's last order from the TSA on Aug. 12 for $54.8 million was the initial order under a new three-year agreement to provide options, accessories, engineering, and installation support for up to 550 units, primarily CTX-9000s. InVision said it expected to ship all units later this year. Upon TSA's previous order in October 2002, InVision said TSA had purchased 625 units since March 2002.

On Sept. 30, TSA said it purchased 43 more L-3 EDS machines valued at $37.84 million, bringing the number of L-3 EDS units purchased to approximately 480.

One of the biggest challenges facing the aviation industry is that U.S.-certified EDS units are not truly *explosives detectors*, but rather are machines that measure the density of objects. Both suppliers have imperfect machinery, which is expected when operating state-of-the-art equipment. Therefore, the machines must be placed into a *process* to determine if the objects are really explosives or harmless items that contain characteristics of explosives materials. Only a properly designed in-line screening system can mitigate most of the technological flaws that become readily apparent when the machines are operated as individual units in ticket lobbies or concourses.

"One system slightly worse than another poor system is not the best purchasing approach, that's for sure," a source familiar with both manufacturers said.

InVision has worked out many of the technical flaws in both its EDS units and the in-line screening process because the firm has benefited from having a longer track record with the first EDS machines and from a wider customer base throughout the world, sources said. In comparison, L-3 has a much smaller working base and Boston is the firm's first large-scale effort to install its machines in a conveyor system. In essence, InVision has worked out some of the kinks L-3 is now experiencing.

Meanwhile, InVision has invested some $25 million in research and development to improve the software packages of their machines, according to the TSA document. The results have been lower false alarm rates and faster throughput rates that are more acceptable to government and airport executives for the widely used CTX-5500s and CTX-9000s, and have thus improved the products' reputations.

"If the L-3 is inferior to InVision technology, Congress never should have directed a one-for-one purchase and, if there are concerns, they need to be resolved before the TSA purchases another $38 million worth of L-3 EDS machines," said Brian Sullivan, a former FAA special agent in New England. "The failed FAA security apparatus had a history of being compromised by the twin hammers of political pressure and adverse corporate influence. I don't want to see more American lives lost because we allow the TSA to do the same thing."

Customer Base Favors InVision

Sources indicate that TSA headquarters has shown little interest – or at the very least has been relaxed – in installing EDS machines in the best possible process. The burden on finding the best possible solution to sufficiently screen baggage while not discomforting passengers and entire airport operations has fallen onto the shoulders of individual airport authorities and their airline tenants. Federal Security Directors (FSDs) at airports are learning the EDS process first-hand and often end up caught in the middle of implementing headquarter decisions and trying to placate airport and airline managers.

TSA officials said in October that no more than 40 U.S. airports will receive letters of intent (LOIs) to assist in funding of in-line checked baggage solutions. An airport receiving an LOI will pay for 25 percent of the project, while the TSA pays 75 percent. To date, only seven airports have received LOIs from the government. In addition, only about a dozen airports have operational in-line systems that will meet the TSA's deadline to screen all passenger checked baggage by electronic means – either with EDS or ETD –

Continued on page 6

by Dec. 31, 2003. Consequently, the majority of those airports building in-line systems will not be bringing those systems on-line until 2004 to 2007.

The TSA's deadline could present problems at some airports. The TSA already has said that five airports will not meet the deadline and, thus, will rely upon other approved screening methods to include hand searches, K-9 inspections and positive passenger bag matches (PPBM).

The overwhelming majority of the 441 airports will permanently depend on EDS units not in a conveyor system or on less reliable ETDs, which are open to inconsistent application during the wanding phase by human screeners. ETDs are not without their own "false alarms" due to hand creams and other miscellaneous organic substances.

Other airports have caught wind of the reliability gap between the two EDS manufacturers.

Spokane International Airport (GEG) CEO John Morrison on Oct. 7 wrote U.S. Sen. Patty Murray (D-Wash.) to request "assistance in contacting the TSA to change the EDS equipment for [Spokane] to the InVision CTX-9000." TSA intended to deploy nine L-3 eXaminer 3DX-6000s, but Morrison said he became aware that Boston and **Tampa International Airport** (TPA) "have experienced significant problems" with L-3 equipment "due to their aperture, throughput and reliability."

The letter, obtained by *ASR*, quoted exact figures from the TSA comparison document of the Boston and San Francisco systems.

In April, Ben DeCosta, general manager of **Atlanta Hartsfield International Airport** (ATL), and 12 airline station managers wrote Willie Williams, TSA's Federal Security Director at Atlanta, to request that the 43 EDS machines destined for the airport are InVision products and not L-3 machines.

The letter referenced InVision's better operational reliability concerning machine aperture, baggage throughput rates and multiplexing capabilities, which diminishes resources needed for labor-intensive secondary screening processes.

"We must strongly object to any equipment allocation plan that will have an adverse operational impact on this critical aviation facility. We urge your support in getting immediate TSA commitment for Hartsfield to be equipped with CTX-9000 EDS units," DeCosta wrote in the letter, obtained by *ASR*.

TSA Administrator James Loy told the House Aviation Subcommittee on Oct. 16 that Atlanta will receive InVision machines. Construction will begin on Atlanta's $215 million system in January and is expected to last 14 months.

The lasting impact of the EDS products' reputations could be in the international arena, where InVision also holds an advantage over L-3's 3DX-6000. While most countries do not demand machines to meet the stricter U.S. certification standards for front-line machines, InVision products have been deployed at international airports in the later stages of screening systems when a more intense bag scan is required.

Canadian officials announced in 2002 that they would adhere to the U.S. standards for bag screening technologies at their airports in the future. The Canadian government did not impose a quick deadline, as U.S. lawmakers did, preferring instead to install the machines into conveyor systems over a few years. Airports are relying on their existing systems, built on European models, until EDS machines are installed.

The European and Asian markets could be key financial regions for the EDS manufacturers as countries may follow U.S. methods in the future if the U.S.-certified products remain the most reliable bag screening machines in the world. While most airports in the past have modeled bag screening systems on European systems, an obvious disparity in standards exists in comparison to the United States. Some major international airports will see the shelf life of their bag screening units expire in the coming years and will face decisions on which technologies to rely upon at the initial phase of screening.

Those markets provide valuable contracts. Sources said there is an intense fight between the manufacturers for the new bag screening system contract at **Bangkok International Airport** (BKK) in Thailand, after L-3 won an exclusive contract in January 2003 for **Singapore Changi International Airport** (SIN) potentially worth $45 million. ✈

International Security

• Australian budget carrier **Virgin Blue** failed to meet a Nov. 1 deadline for the installation of reinforced cockpit doors on its aircraft, according to Australian officials. Australia's **Transport Department** extended the deadline for the carrier to March 2004. Virgin Blue had difficulty acquiring the new hardened doors from its supplier. Meanwhile, **Qantas Airways** [PNK: QUBSF.PK] complied with the order on all except one airplane, which required extra maintenance work after flying through a storm. ■

TSA Effectiveness Doubted Over Lack Of Screener Testing

The **Transportation Security Administration** (TSA) performed covert tests at airports on less than 1 percent of its workforce from September 2002 to September 2003, a congressional investigator told the **U.S. Senate Committee on Commerce, Science and Transportation** on Nov. 5.

TSA has collected "limited information on the effectiveness of its aviation security initiatives" in the first year since some 50,000 airport security screeners were deployed at 441 airports, said Cathleen Berrick, director of homeland security and justice issues for the **General Accounting Office** (GAO).

Federal aviation investigators attempted to take threat objects past security checkpoints in covert tests only 733 times at 92 airports, Berrick said. Additionally, TSA's internal affairs office conducted about 2,000 access control tests to restricted areas, but only 168 Computer Assisted Passenger Pre-Screening System (CAPPS) and checked baggage tests.

TSA deputy administrator Stephen McHale said another 100 checkpoint tests and more access control tests have been performed in the past two months. McHale defended TSA's lack of screener performance data by saying, "We are conducting covert testing at over three times the annual rate of the old [**Federal Aviation Administration**] 'red teams,' and our testing uses more difficult, realistic testing situations."

McHale said the agency's focus in its first 14 months was to create the agency and meet congressional mandates to deploy personnel and equipment at airports. "Having done that, we are now very much focused on measuring our performance and moving forward with that," he said.

But a congressional leader chastised the TSA for not knowing their strengths or weaknesses.

"What I am concerned about concerns Ms. Berrick's testimony and what I've been told is a lack of measures of TSA screening effectiveness," said Sen. John McCain (R-Ariz.), chairman of the committee. "I don't know how we make progress or can know what areas need to be improved unless we have some measures of determining what progress or lack of progress is being made, where our failings are."

McCain said measuring the system's effectiveness could lead to significant improvements in technology that could restore confidence to the flying public. "We need technology. We predicted a long time ago that we would have some kind of system where people who are, quote, 'trusted' could move right through," he said. "I can't see, frankly, from my eyesight any significant improvement in the process that passengers go through since the day that these procedures were installed."✈

In-Line Done Right

The Jacksonville Airport Authority and the Airport Consultants Council invite you to attend Hold Baggage Screening (HBS) System Workshop & Demonstration at the Jacksonville Airport (JIA), December 8-9, 2003. This two-day symposium will feature presentations on the planning, designing, and operating an In-Line HBS System, and a tour of the automated the standard for HBS

Participants will

- System design
- Space
- Integrating TSA
- Operational and staffing considerations and
- Maintenance requirements and
- RFID

You won't want to miss this opportunity to learn JIA's experience in how to create solutions to your airport's baggage check-in security

Contact Cassandra Lamar, ACC, at cassandral@acconline.org or 703.683.5900, for registration, exhibiting, and sponsorship information.

ASR's BREACH REPORT

DATE & SITE	AREA*	CIRCUMSTANCES	RESULT
October 9 – Baltimore-Washington Int'l Airport (BWI)	3	A screener at checkpoint D observed the outline of a long-barreled gun on the monitor of an X-ray machine.	Screeners closed the checkpoint and called **Maryland Transportation Authority** police to the scene. Police arrived and took the man and his carry-on item to an airline ticket counter. The item was scanned by an explosives detection system. The gun outline turned out to be a BB gun. The man was allowed to keep the gun in the bag and the bag was treated as a checked bag. The man was allowed to board his flight. No flights were delayed.
October 11 – Dunedin Airport, New Zealand (DUD)	2	**Air New Zealand** staff noticed an unattended bag in front of a ticket counter.	Police evacuated and cordoned off the southern end of the airport terminal. Two flights were forced to disembark on the tarmac. The backpack was searched and nothing suspicious was found. A man who boarded a flight to Auckland forgot the backpack.
October 12 – Ottawa Int'l Airport, Canada (YOW)	Customs	About 200 passengers arriving from London walked off **Air Canada** Flight 889 and roamed undetected in the terminal and unchecked by Customs agents.	Some passengers were able to enter the main terminal and mix with domestic flight passengers waiting for their luggage at baggage carousels. Customs agents learned about the security breach only after a passenger let them know. Passengers were recalled over the public address system. Agents fanned out into the terminal and escorted passengers back to examination areas. Other passengers returned voluntarily. It is believed all passengers were accounted for. Confusion regarding the layout of the new terminal is being blamed for the mishap. It was opening day for the new terminal. Passengers apparently walked down the wrong corridor from the boarding gate and into a public area serving domestic passengers instead of going down an escalator toward immigration and customs.
October 15 – Edinburgh Airport, Scotland (EDI)	3	A man ran from the baggage carousel area up a flight of stairs, past a security checkpoint and into the first floor departure lounge.	Airport staff pursued the man but was unable to find him in the crowd. The concourse area was evacuated around 6:30 p.m. Two planes were already boarded. They were evacuated and searched before all passengers were allowed back into the concourse. About 1,000 people were evacuated and rescreened. The man was not found.
October 15 – San Diego Int'l Airport (SAN)	8	A man drove a late model sports car through two perimeter security fences, and then onto the airport tarmac.	The man bailed out of the moving car before running back under the fences. He was captured without incident moments later by Marines stationed as guards at the nearby **U.S. Marine Corps** Recruit Depot. The car continued to move at a slow rate of speed across the tarmac, crossing the airport's only runway before running into a fence on the far side of the field. No one was endangered by the incident, and no planes taking off or landing had to be diverted. A canine unit checked the car to make sure there were no explosives in it. No weapons or explosives were found.
October 16 – New Orleans Int'l Airport (MSY)	6	A pilot reported a rear lavatory problem during the late afternoon on **Southwest Airlines** [NYSE: LUV] Flight 474.	Technicians found a collection of items behind an access panel. The items included two ash-colored box cutters, each complete with blade, approximately 10-12 oz. of a simulated plastic explosive (reddish molding clay), a few dozen strike-anywhere matches, and approximately 8 oz. of liquid bleach. A note stated the items were taken through a security checkpoint at **Raleigh-Durham International Airport** (RDU) and placed aboard the plane on Sept. 12. *(Note: This is the fifth of Nathaniel Heatwole's six incidents.)*
October 16 – Houston Hobby Airport (HOU)	6	At approximately 11:15 p.m., a routine maintenance check of the rear lavatory uncovered a package of items.	The package contained three ash-colored box cutters, each complete with blade, approximately 10-12 oz. of a simulated plastic explosive (reddish molding clay), a few dozen strike-anywhere matches, and approximately 8 oz. of liquid bleach. An anonymous note said the items were taken through a security checkpoint at **Baltimore-Washington International Airport** (BWI) and placed aboard the plane on Sept. 14. Southwest Airlines contacted the **Transportation Security Administration** (TSA). *(Note: This is the sixth of Nathaniel Heatwole's six incidents and subsequently led to his arrest for carrying a concealed dangerous weapon onto an aircraft.)*

* - Codes where security incident took place:
1 – Roadway/parking lot/off airport 2 – Public ticket lobby/baggage claim 3 – Security checkpoint
4 – Sterile concourse/gate area 5 – Checked baggage/cargo x-ray examination 6 – Inside aircraft
7 – Airside operations area 8 – Airport perimeter *Compiled by ASR from various news sources*

Post-Hearing Questions Submitted by Senator Susan M. Collins,
Chairman, Senate Committee on Governmental Affairs
for the Nomination of James M. Loy to be
Deputy Secretary of Homeland Security

Interoperability

Question 1: This year, the Department of Homeland Security and the Department of Justice developed a Joint Interoperable Communications Initiative to coordinate their separate interoperability grant programs. Instead of providing seed money to a number of communities, these programs gave a significant amount of funding to only a few areas. This approach left over a hundred candidates -- including two Maine cities, Portland and Bangor – without funding. Applying FY2004 interoperability funding to existing applications would avoid forcing communities to reinvent the wheel by having to complete yet another application or homeland security plan. Would you consider allocating a portion of the 2004 interoperability funding to cities that applied but did not receive funding this year?

Answer: Under the FY 2003 Consolidated and Supplemental Appropriations, EPR received $79.75 million for grants for interoperable communications. The Department of Justice, Office for Community Oriented Policing Services (COPS), also received funding for interoperable communications grants. EPR worked closely with COPS to implement a coordinated competitive demonstration grant program. This grant program provided funding to local jurisdictions for demonstration projects that will explore the uses of equipment and technologies to increase interoperability amount the fire service, law enforcement, and emergency medical service communities. DHS did not receive FY 2004 funding for the Interoperable Communications initiative. The Department of Justice (COPS) Office has not yet received its FY 2004 appropriation, so it is unclear if this initiative will be funded in FY 2004.

In FY 2004, the Department's two primary programs that support state and local interoperability efforts are the Homeland Security Grant Program (HSGP) and the Urban Areas Security Initiative (UASI). Both of these programs are administered by the Department's Office for Domestic Preparedness. Under HSGP, the Department is allocating $2.2 billion to all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and the territories to support state planning, management and administrative efforts, training and exercise programs, equipment acquisition, including interoperable communications equipment. Under UASI, the Department is providing $675 million for 50 urban areas to support domestic preparedness efforts. Like HSGP, UASI funds can be used by the designated urban areas to enhance their communications interoperability. For both programs, the ODP provides comprehensive guidance on the development of interoperable communications plans.

Question 2: The Joint Interoperability Communications Initiative also focused primarily on large urban areas. Many rural areas also face serious threats, such as agroterrorism, and vulnerabilities, such as borders and coastlines. They also face very different interoperability challenges, such as a scarcity of few existing cellular towers that must cover expansive areas.

What steps will you take to ensure that the Department also finds interoperability solutions for rural areas?

Answer: The pool of nominees invited to submit applications for the FEMA/COPS grant program were culled from three primary sources. The fifty largest Metropolitan Statistical Areas (MSAs) in the country, as well as the largest MSAs from each respective state were invited to apply for the COPS's portion of the funding. In addition, governors from each state were asked to nominate a local jurisdiction to submit an application for an interoperable communications demonstration project to apply for FEMA's portion of the funds. As part of these nominations, governors were encouraged to consider opportunities for innovative and inclusive approaches to achieving interoperability among the public safety community, including regional or other partnerships that cross jurisdictional boundaries. While the COPS applicants represented the largest metropolitan areas, FEMA's applicants and grant recipients represent a variety of demographics, including rural areas. FEMA and COPS recognized that the interoperability needs of a rural area might be different than those of a large city. The recipients of the DHS/FEMA FY 2003 Interoperability Communication Grants included rural areas.

In FY 2004, the Department's two primary programs that support state and local interoperability efforts are the Homeland Security Grant Program (HSGP) and the Urban Areas Security Initiative (UASI). Both of these programs are administered by the Department's Office for Domestic Preparedness. Under HSGP, the Department is allocating $2.2 billion to all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and the territories to support state planning, management and administrative efforts, training and exercise programs, equipment acquisition, including interoperable communications equipment. Under UASI, the Department is providing $675 million for 50 urban areas to support domestic preparedness efforts. Like HSGP, UASI funds can be used by the designated urban areas to enhance their communications interoperability. For both programs, the ODP provides comprehensive guidance on the development of interoperable communications plans.

The Department recognizes the need for predominantly rural and agricultural areas to conduct similar analyses of threats and vulnerabilities to possible terrorist attacks. To meet this need, the Department significantly updated its State Homeland Security Assessment and Strategy (SHSAS) process to incorporate a suite of assessments focused on agricultural vulnerabilities and response capabilities to WMD incidents involving agricultural resources. As you know, the SHSAS process and resulting state homeland security strategy are a requirement of states' receiving their FY 2004 Homeland Security Grant Program allocation. The assessment information and strategy information will be used by the states to determine how they will use their homeland security funds, including how these funds can be used to support preparedness efforts in rural areas.

The optional agricultural assessment component of SHSAS was developed in coordination with the U.S. Department of Agriculture for state use, and addresses potential agricultural targets, agricultural planning factors, and current and desired agricultural response levels. There are also agricultural components included in the planning, organization, equipment, training, exercises, and technical assistance portions of the basic SHSAS process. Jurisdictions within the state that

have substantial agricultural industry resources, activities, or enterprises, are encouraged to complete the agricultural component in addition to the basic assessment. States/jurisdictions that wish to complete the agricultural assessment are encouraged to establish an agricultural working group comprised of experts who understand the complexities of the agricultural industry.

The optional Agriculture Vulnerability Assessment provides an opportunity for states/jurisdictions to assess potential agricultural targets (through the evaluation of the target's level of visibility, criticality of the target, impact on the agricultural industry, access by a potential threat element to the target, capacity of the agricultural facility, and the product distribution area).

Coordination of Grant Programs

Question 3: A recent report by the Department's Office of Inspector General found duplication and overlap between federal homeland security grant programs and called for more coordination. This report looked at two grant programs and found duplication for more than 113 distinct items, such as interoperable communications equipment and personal protective equipment. Recipients of these grants, however, are not required to declare other federal funding sources. This information could be very useful to make sure equipment purchased with federal funding is interoperable and prevent duplication of assistance. I realize that the Department has now established a single web site for homeland security grant programs, but would you also support efforts to require recipients to notify federal agencies if they receive supplemental funding from another federal agency?

Answer: The Department of Homeland Security is committed to providing resources and assistance to states and localities in the most efficient and effective manner possible. The Department recognizes that in order for state and local jurisdictions and first responders to be effective partners with the federal government in securing our homeland, they need quick and easy access to the terrorism and emergency preparedness grant programs designed to support their work.

DHS is convinced that these programs must be more centralized and more accessible. It is our goal to provide state and local authorities a single point of contact for terrorism and emergency preparedness efforts – one access point to obtain critical grant funding. The Department's recent announcement of a "one-stop-shop" application for three different programs administered by the Office for Domestic Preparedness is a important step in this direction. The single application allows states to apply online for their allocated grants that benefit first responders and will provide additional resources to state and local government counterterrorism efforts.

This consolidation was done to streamline the grant application process and better coordinate federal, State and local grant funding distribution and operations. The homeland security assessments and strategies currently being finalized by the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, U.S. territories, and selected urban areas for submission to DHS-ODP will play a pivotal role in the identification, prioritization, and allocation of financial

resources provided through the three grant programs. The funding provided will be applied against critical resource gaps identified through the assessments and prioritized in the State strategies.

Providing funds through a single application and award process facilitates coordination of preparedness activities related to the goals and objectives identified in the State strategies, resulting in a more effective and efficient use of funding. A single application also minimizes time spent on the application process and consolidates reporting requirements.

In addition to the single application, DHS is launching an interagency grants and training website on the DHS website at www.dhs.gov/grants. The website provides information on homeland security and public safety grant opportunities offered by DHS and other federal departments and agencies including HHS, DOJ and the EPA. It also provides a link to the Compendium of Federal Terrorism Training for State and Local Audiences, an interagency site for training opportunities available to state and local emergency personnel.

Student Exchange and Visitor Information System (SEVIS)

Question 4: The Internet-based Student Exchange and Visitor Information System (SEVIS) is designed to collect, maintain and manage information on international foreign students, exchange visitors, and their dependents during their stay in the United States. SEVIS was designed to improve the process through which foreign students and exchange visitors gain admission to the U. S. I understand that foreign applicants are limited to the SEVIS list of approved schools. I understand that all schools on this list are required to have approval or certification by the Student and Exchange Visitor Program (SEVP). If a student enrolls in a school that is not included on the SEVIS list, the State Department will not issue him or her a visa. What worries me is that there is currently no requirement for schools on the SEVIS list to be accredited by an agency that is recognized by the Department of Education. Without requiring Department of Education-recognized accreditation, how can the Department ensure the legitimacy of schools on the SEVIS list? For that matter, how can you be certain that a foreign student could not secure a student visa by enrolling in a diploma mill on the SEVIS list?

Answer: Starting in October 2002, as stipulated by law, all schools that enroll foreign students have been required to receive approval or certification by the Student and Exchange Visitor Program (SEVP). Certification verifies their knowledge of the requirements of SEVP and how to employ the Student and Exchange Visitor Information System (SEVIS). The primary regulation that determines the basis for school certification is 8 CFR 214.3 Approval of schools for enrollment of F and M nonimmigrants. It cites four general criteria for approval of schools [8 CFR 214.3 (e) (i-iv)]:

(i) It is a bona fide school;
(ii) It is an established institution of learning or other recognized place of study;
(iii) It possesses the necessary facilities, personnel, and finances to conduct instruction in recognized courses; and,
(iv) It is, in fact, engaged in instruction in those courses.

Many schools receive accreditation from academic or professional associations. That accreditation certifies that the four criteria (above) are met. In these cases, SEVP is required to verify that an applying school has current accreditation. SEVP must keep some documentation on file related to how the school met that accreditation.

For those schools not accredited by an academic or professional association, the SEVP certification process must replicate the accrediting function. Consequently, the SEVP certification of schools in this group requires more documentation and the process is more complex.

Beyond the issue of accreditation, SEVP certification must clearly establish that the applying school:

- Understands the national security need for compliance with SEVP;
- Has necessary computer hardware, is competent with the SEVIS software, and is able to interact effectively with students, other schools, and SEVP through the SEVIS database;
- Is knowledgeable of the requirements that the SEVP places on the school, as enumerated in 8 CFR 214.3; and,
- Recognizes potential consequences to the student, the school, and the nation by failing to comply with these requirements.

Regarding schools without accreditation from academic or professional associations, experience since October 2002 has demonstrated that truly bona fide schools, irrespective of their accreditation, have received certification.

SEVP is confident that all SEVIS certified schools have met the legal requirements of that recognition. However, we actively seek to improve the effectiveness of the certification process. Consequently, as of November 1, 2003, processing and adjudication of I-17 school certification applications have been centralized at the SEVP office in Washington, D.C. This movement reflects a clarification of responsibilities among elements of the former Immigration and Naturalization Service that have been relocated within two agencies of the Department of Homeland Security (DHS), i.e. the Bureau of Citizenship and Immigration Services and the Bureau of Immigration and Customs Enforcement. More importantly, this action is being taken to establish a full-time, professional work force that will be dedicated solely to accomplishing this critical certification process.

Consolidation will enable SEVP to better standardize the application of adjudication criteria and to institute efficiencies that will more closely serve the needs of academic institutions while protecting Homeland Security.

As of February 15, 2003, all students or exchange visitors must present a valid SEVIS I-20 or DS-2019, as applicable, to Department of State (DOS) personnel at a U.S. embassy or consulate in order to receive a visa. These documents are provided to the student or exchange visitor directly from the school or program where the student intends to enroll. Only SEVIS certified

schools and exchange visitor programs can issue these forms. A number of alternate forms of identification are also required in order to confirm that the person who possesses the SEVIS document is, in fact, the person registered in SEVIS. As a backup to this procedure, DOS personnel have alternate means to affirm the SEVIS status of the individual applicant. Should circumstances indicate a need for further confirmation, DOS officials can contact SEVP headquarters, as well as the sponsoring school or program, for further clarification. Additionally, SEVIS documents include bar-coding encryption, which makes the documents resistant to unauthorized duplication.

TSA Screeners

Question 5: The recent case involving college student Nathaniel Heatwole raises a number of questions about the effectiveness of TSA screening procedures. Mr. Heatwole was able to smuggle box cutters and other contraband aboard six airplanes, and left these items on four airplanes. Even worse, his e-mailed warning to TSA was ignored until an airplane maintenance worker discovered some of the items he had hidden on a plane. These facts make me wonder about the effectiveness of passenger screening, of the airlines' daily inspections of their aircraft, and of TSA's complaint center, which received Mr. Heatwole's warning. TSA has begun an investigation of this matter. What shortcomings have you found, and how are they being corrected?

Answer: I recently approved a short-term screener performance improvement plan that includes several training components. The overall plan consists of a series of immediate, 6-week, 3-month and 6-month milestones leading to full implementation by March 31, 2004. Specific training initiatives include: 1) Acceleration of leadership training for all screening supervisors; 2) Development and implementation of an advanced technical course for screening supervisors; 3) Full implementation of a recurrent training program for all screeners and screening supervisors; 4) Deployment of Modular Bomb Sets and weapons kits to all airports for local training; 5) Implementation of an on-line image interpretation training module for all screeners and screening supervisors; and 6) Full implementation of the Threat Image Projection (TIP) system. TSA's commitment is to continuous learning and to always gain insight from our covert test results to continuously raise the bar on screening performance. As an added measure, TSA has created a set of x-ray images depicting items similar to those carried by Mr. Heatwole and distributed those images to the screener workforce for training purposes.

In addition, the channel through which TSA received the email needed additional attention. TSA's Contact Center has been the focal point for receiving comments on travelers' experiences in screening and for reporting lost or damaged property, but not for receiving security alerts. The Contact Center receives an average of more than 5,000 telephone calls and e-mails each week, the vast majority reflecting the types of concerns noted above. The email that TSA received through this channel was not viewed as a threat, but clearly it should have received priority treatment as a potentially serious message involving security information and illegal activity.

TSA has swiftly changed procedures at its Contact Center and throughout TSA. Contact Center

electronic mail, telephone calls, and other communications are now filtered for security content, reviewed by a security analyst, and when appropriate, transmitted to our Transportation Security Coordinating Center and other units for action. Contact Center personnel are trained each month on how to identify potential security violations, threat information, and criminal activity conveyed through telephone calls or other means. In addition, all TSA employees and contractors have been given specific protocols to follow in identifying, documenting, and reporting potential threat communications.

Procurement

Question 6: I am concerned by complaints that I have received about the Department of Homeland Security purchasing goods and services without using full and open competition, in particular at the Bureau of Customs and Border Protection. As a strong advocate of full and open competition, I would hope that these complaints are unfounded.

- First, do you share my views that contracts should generally be awarded with full and open competition?

Answer: Yes, DHS strongly advocates the use of full and open competition; however, there may be circumstances where another allowable procurement process is justified. These instances should be the rare exception rather than the norm.

- Next, if confirmed, will you promptly provide us with a breakdown of the number and amount of contracts within the Department that are awarded through full and open competition and those awarded using less competitive procedures?

Answer: Yes, DHS will provide competition statistics for all contracts awarded by the Department as of the date DHS was established, 1 March 2003, through the end of the fiscal year.

Port Security

Question 7: Last month, the Coast Guard published the final rules for implementation of the Maritime Transportation Security Act of 2002. The Coast Guard has estimated that the cost of complying with these new regulations will be $1.5 billion the first year and $7.33 billion over the next 10 years. Do you think the Administration should include funding for the port security grants in the 2005 budget?

Answer: Implementation of the Maritime Transportation Security Act of 2002 is a priority, not only for DHS, but for all the state, local and private sector entities which share this responsibility. Through this public-private partnership, all of the entities at our nation's ports have born and will continue to address the costs of necessary security improvements. Although the FY 05 budget decisions are pre-decisional, the Department believes that port security grants are an appropriate mechanism to fund some of the requirements of MTSA implementation. The Department will continue to assess our nation's vulnerabilities and assist states and localities in

protecting our critical infrastructure.

Question 8: The Coast Guard is in the process of conducting port vulnerability assessments at the nation's 55 military and strategic ports. I am told that a total of 15 of those assessments will be completed by the end of November. The Coast Guard is scheduled to complete all 55 assessments by the end of 2004. How has the port security grant selection board been able to effectively evaluate the needs of applicants when in some port areas the Coast Guard vulnerability assessments have not been completed?

Answer: The Port Security Grant program has been administered through a rigorous, multi-tiered evaluation process of competitive grant applications, involving the U.S. Coast Guard, TSA and the Maritime Administration (Department of Transportation). The Port Security Grant Program evaluation process incorporates a multi-level, interagency review which includes: a *local/regional review* by Coast Guard (USCG) Captain of the Ports and Maritime Administration (MARAD) Regional Directors to verify applicant eligibility and rank applications based on risk/mitigation; a concurrent *State level review,* where designated State Representatives may elect to review and prioritize grant applications received from their respective states; a *national level review* which consists of technical subject matter experts from the three agencies (USCG, MARAD and TSA); and an *executive review,* where agency representatives from USCG, MARAD, and TSA evaluate the proposed grant awards from an overarching national perspective. The *selection board,* which consists of the Administrator of the TSA, the Administrator of the MARAD, and the Commandant of the USCG (or their representatives), makes the final award selections. Because of the robust and layered evaluation process, sufficient information is available for evaluators of grant applications to make award determinations.

Question 9: After the second round of grants was awarded this past summer, some observers were surprised to see that several private entities had been awarded disproportionately large amounts of funding. For example, a CITGO oil facility in Lake Charles, Louisiana, received a grant of more than $13 million. The entire state of Maine received less than $1.3 million. How do you explain such a large distribution to just one private facility?

Answer: Port security remains a shared public/private responsibility, and the government currently awards grants to both. TSA's competitive Port Security Grant Program provides federal assistance to critical national seaports for security enhancements identified in security assessments. The application process, as described above, is based on national security priorities and sound criteria.

Question 10: The Maritime Transportation Security Act of 2002 regulations are scheduled to go into effect on November 22, 2003. They will apply to approximately 10,000 domestic ships and 5,000 waterfront facilities. The Coast Guard has estimated that these maritime stakeholders will spend more than $1.3 billion in the first year alone to comply with the regulations and make the necessary security upgrades. Maritime officials have expressed concern over the costs and have

been seeking relief through the port security grants program. Do you think competitive grant programs are the best way to offset port security costs for the maritime industry?

Answer: The security of our nation's ports is a high priority, and the Department appreciates the support of our public-private partners in working together to address identified vulnerabilities. As the responsibility is shared so too are the costs. Federal, state, local governments as well as the private sector entities in the port community all have a role to play. The Coast Guard, in the person of the Captain of the Port, provides federal leadership at the local level in this effort, working in close partnership with the port authority and any number of local players. DHS presence also includes the work of Customs and Border Protection in cargo and container security. Both these agencies represent a significant federal commitment to security at our nation's ports. Furthermore, DHS support of state and local first responders assists overall preparedness, including at our nation's ports, in the event of natural disasters or terrorist acts.

The port security grant funding provided in the last two years has been awarded to mitigate some of the costs born by the maritime industry. Grants provide a structured mechanism for allocating resources to address national priorities and mitigate vulnerabilities such as those identified by the port security assessment program. They represent one effective tool the Department has to further strengthen our nation's security.

Question 11: The Coast Guard is expecting some 10,000 security plans to be submitted by vessels and facilities for review and approval beginning next year. The Coast Guard's Commandant has estimated that this oversight program alone will require $70 million and 150 full-time personnel. To date, no funding has been appropriated for implementation of MTSA. How is the Coast Guard absorbing this extra workload without additional resources and do you think additional funds for this purpose would be helpful?

Answer: First, let me assure you that complying with the requirements of the MTSA is one of DHS' highest priorities and essential to demonstrating the U.S. commitment to Port Security.

While the Coast Guard's FY04 Appropriation does not include funding for vessel and security plan review, not all aspects of the MTSA have been unfunded. For example, the Coast Guard's FY04 Appropriation contains nearly $100M for items specified in the MTSA such as Maritime Safety and Security Teams, Automated Identification Systems, and positive vessel control activities (previously called Sea Marshals). The Coast Guard's FY04 Appropriation also contains another $88M in new boats, cutters, and shore station infrastructure that will be used to enhance the security of the marine transportation system. This, however, does not fully fund MTSA implementation.

The Coast Guard will also internally reprogram resources as necessary in FY04, but at a cost to other critical initiatives. The details of the reprogramming will be outlined in the Coast Guard Fiscal Year 2004 Final Operating Stage Financial Plan that will be provided to Congress. We are also working with the Administration to ensure appropriate resources are included in the FY05 budget submission.

Question 12: I understand that TSA has been testing different ID card technologies in recent months that can be used to manage transportation worker access into secure transportation areas and operations. The Transportation Worker Identification Card, or TWIC program, is expected to provide one standardized, common credential tied to a single integrated and secure network of databases. What are your next steps with this program and how long before we can expect it to be implemented nationwide?

Answer: Phase I of development of the TWIC program, the planning phase, was completed in March of 2003.

The Technology Evaluation (Phase II) was completed October 21, 2003. The intent of the Technology Evaluation Phase was to evaluate a range of potential card technologies as they relate to credentialing and their applicability to access control at various transportation facilities in the Philadelphia / Delaware River Basin and Los Angeles / Long Beach areas (regional pilots). The final report was delivered November 7, 2003.

The TWIC program office will begin the Prototype Phase (Phase III) in the early 2004 timeframe. Its purpose will be to validate technologies identified in Phase II across a broad range of business processes as they relate to credentialing, identity and identity management, including; verification of claimed identity, enrollment procedures and background checks. In addition, the Prototype Phase will introduce and test biometric technology, as well as contactless technology. Phase III will be conducted at select facilities that participated in the regional pilots. Additional sites may be added for modes or regions that currently require a background check by statute or regulation. The Prototype Phase will last approximately seven months.

Subject to congressional approval, implementation (Phase IV) is expected to begin around mid to late 2004 and full implementation is expected in 2007.

CAPPS II

Question 13: Admiral Loy, I understand that TSA's Office of National Risk Assessment (ONRA) has been given the responsibility for development of the CAPPS II program. Do you envision the technologies, policies and programs developed by ONRA for CAPPS II being used for other homeland security efforts that would benefit from having a threat-based risk assessment engine? What steps is the Department taking to ensure that the information systems it builds are flexible enough to be adapted to new purposes so that substantially similar systems are not built from scratch when the need arises?

Answer: One of the goals of the Information Analysis and Infrastructure Protection Directorate is to leverage existing capabilities while also identifying new requirements in threat based risk assessment tools, and working in concert with the Office of the Chief Information Officer to identify or build those capabilities. IAIP and CIO are currently evaluating all of the Department's available tools and resources for performing risk assessments, to include the engine under development for TSA's CAPPS II system, for use in other Homeland Security efforts that would benefit from having a risk assessment engine.

Post-Hearing Questions from Senator Joe Lieberman
for the Nomination of James M. Loy
to be Deputy Secretary of the Department of Homeland Security

Question 1: TSA this year reduced its screener workforce by a total of 6000 positions. Yet there are deeply troubling indications that TSA does not have enough screeners in place, and is having trouble retaining screeners. For instance, in a report carried on Boston-area public radio station WBUR on November 18, 2003, the Federal Security Director (FSD) at Boston's Logan Airport complained about the high rate of attrition in its screener workforces, stating the airport has lost roughly one-third of its screener workforce in the last several months and is currently understaffed. The WBUR report also cited a June 2003 e-mail from the FSD at Dulles Airport, which reportedly stated that, at that time, only 57% of bags at that airport were being screened electronically because of serious screener staffing problems. You yourself have raised concerns about screener staffing levels. In testimony before the Senate Commerce Committee on September 10, 2002, you urged lawmakers to reconsider the limit of 45,000 full-time employees imposed by the [FY 03] supplemental." Also, in response to Question #14 of my pre-hearing questions, you indicated that "[s]everal of the airports using non-electronic screening methods are doing so due to screener workforce shortages." In response to that same question, you indicated that TSA will be seeking money for additional screeners in an FY 04 supplemental request.

Please state how many screeners you believe are needed for TSA to fulfill its security mandate. What are the budget implications of fully funding these requirements? Specifically with respect to the FY 04 supplemental request, please state how many additional screeners TSA may seek authorization to hire and over what period.

Answer: The challenges in achieving the optimized quantities of screeners vary considerably from airport to airport. DHS, TSA and OMB are continuing work to maximize available resources against the many needs of transportation security in order to arrive at an acceptable figure.

While it is true that the overall size of the workforce is declining, TSA is creating additional capacity through achieving greater efficiencies in the scheduling of screeners. Federal Security Directors (FSD) at each airport now have access to scheduling tools that provide real-time information enabling them to forecast periods of peak demand for screening. TSA uses more split shifts and part-time screeners to maximize the operational flexibility available to FSDs when scheduling screeners to satisfy varying levels of demand. As a result of reducing excess capacity at periods of lower demand, fewer FTE can be used to meet the workload. This flexibility will allow TSA to meet the demands of its security mandate.

- Additionally, how do you assess TSA's record at retaining qualified screeners and what improvements, if any, are needed to combat attrition?

Answer: I believe TSA is doing an excellent job at retaining qualified screeners. TSA's attrition rate is roughly 13.6% (2003). This stands in contrast to the workforce responsible for U.S.

airport security screening before the creation of TSA whose attrition rate was over 100%. Screeners employed by the airlines, often through contracts with private companies, received minimal training and were often poorly motivated. Contract screening forces were plagued with high rates of attrition that resulted in an average screener tenure of 4.5 months, making it all but impossible to develop and maintain the consistent level of proficiency required to ensure reliable screening.

Maintaining a high level of screener proficiency requires constant diligence. In July of this year, TSA conducted a Screener Performance Improvement Study to determine the root causes for deficiencies in screener performance. After identifying the desired level of screener performance, data gathered from multiple sources was used to determine the actual, current level of performance and the root causes for the gap between desired and actual performance. Based upon this study, TSA has identified an array of solutions and are in the process of further evaluating and implementing them.

Two important elements of TSA's plan for screener improvement are recurrent screener training and supervisory training. Recurrent training is needed to maintain and enhance the skills of screeners, particularly in the areas of x-ray image interpretation, the search of persons, and the inspection of property. Supervisory training will enhance leadership skills in our workforce and provide the advanced technical skills needed to adequately supervise the screening process and resolve alarms.

Question 2: In the WBUR story, security officials at Logan Airport also suggested that TSA's structure is "overly centralized" and does not allow local security officials sufficient flexibility to make hiring and staffing decisions to meet their needs. Are you aware of these concerns? How is TSA hiring screeners to replace those who have left through attrition? Is this hiring being done in a centralized fashion by TSA headquarters or are local airports being allowed to conduct hiring to meet their staffing needs? Who decides how many screeners are needed at each airport and the number of full- and part-time screeners at each airport, TSA headquarters or each airport? What input do FSDs have into the screener staffing and hiring process, particularly at Category X airports?

Answer: Based on the model TSA developed to determine the number of FTEs needed at each airport, each FSD is provided with a specific allocation of FTEs. FSDs are responsible for determining the mix of full-time and part-time screeners that will be needed to satisfy security needs at their respective airports. If an FSD determines that additional part-time screeners are needed to fill any vacant positions, the FSD notifies his/her respective Area Director (in the Aviation Operations office), who prioritizes the requirements of individual FSDs with all screener hiring requirements and available funding. The Aviation Operations office then works with the TSA Human Resources office and the HR services contractor to recruit qualified persons to fill the vacancies. The goal is for FSDs to have sufficient numbers of part-time screeners available to meet screening demands during periods of heavy passenger flows.

The Federal Security Directors (FSDs) are currently being provided with the Sabre scheduling software program that directly interfaces with airline schedules. This provides a method for

ensuring the necessary staffing at each screening operation. To help achieve the right mix of part-time and full-time screeners at each airport, TSA has initiated a process to solicit screeners to volunteer to convert from full-time to part-time employment. In addition, at some airports that need to reduce the number of full-time employees, but do not have a sufficient number of volunteers for part-time employment, some screeners will be either involuntarily converted to part-time status or will be released from employment. All new screeners brought into the screener workforce will be hired as part-time employees, and will later be offered full-time employment, if and when, such opportunities become available.

Question 3: With respect to the FY 04 supplemental request, what other funding needs – in addition to the screener request – may TSA include in that request?

Answer: DHS, TSA and OMB are working to develop a funding strategy to meet TSA's needs in fulfilling its transportation security responsibilities. At this time, it would be inappropriate to comment on what the Administration might ask for in a Supplemental request.

Question 4: As you know, there have been numerous allegations of waste and abuse regarding a contract between TSA and NCS Pearson for the hiring of screeners. According to reports, the original amount of the contract was for $104 million, but the final cost ballooned to roughly $700 million. Are these allegations correct? If so, please explain why the cost of this contract so vastly exceeded original estimates. Do you believe there was wasteful or inappropriate spending by NCS Pearson? What will TSA and DHS do to ensure that future contracts are closely monitored and taxpayer dollars are wisely spent?

Answer: There were many reasons for the cost increases in the NCS Pearson contract. The DHS Inspector General's Office is reviewing the larger TSA contracts awarded to accomplish TSA's mission included in the Aviation and Transportation Security Act to determine what could have been done differently and recommend how similar problems could be avoided in the future. In addition, the Defense Contract Audit Agency is conducting an audit of NSC Pearson invoices. A draft audit report is expected to be completed soon. TSA has not made payment on several NCS Pearson invoices pending completion of that audit.

As mentioned, TSA is drawing on the knowledge and expertise from the Defense Contract Audit Agency and Defense Contract Management Agency, in addition to program support contractors to support and strengthen the contract oversight functions. For example, the Defense Contract Audit Agency has performed approximately 133 individual contract audits on our behalf.

TSA is currently utilizing the Defense Contract Management Agency to support our contract administration in 6 functional areas:

- pre-award pricing,
- earned value management,
- property administration,
- contract close out,
- contractor system reviews
- contract definitizations

TSA employs the services of commercial organizations in support of contract oversight and internal controls. There is an individual in our Office of Acquisition that manages the Contract Audit and Administration programs. This individual's primary responsibility is:

- To ensure that the appropriate contractor systems, pricing proposals, contracts, and modifications are reviewed by the DCAA and DCMA.

Post- Hearing Questions from Senator Durbin
Strategic Planning for Homeland Security
Measuring Performance

One of the tasks the Department of Homeland Security is tackling is developing a Department-wide Strategic Plan. I understand the Department is designing goals, objectives, timelines, and performance measures to analyze and be able to report annual or other periodic progress on how well the Department is meeting its statutory mission.

The primary mission of the Department of Homeland Security, codified at 6 USC §111(b), is to-

(A) prevent terrorist attacks within the United States;
(B) reduce the vulnerability of the United States to terrorism;
(C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States;
(D) carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning;
(E) ensure that the functions of the agencies and subdivisions within the Department that are not related directly to securing the homeland are not diminished or neglected except by a specific explicit Act of Congress;
(F) ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland; and
(G) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking.

Question 1: How is the Department addressing the challenge of designing performance measures and gathering data to determine whether its programs have demonstrated success or made improvements in "prevention", "reduction" and "minimization" of terrorism, which may prove complicated to quantify? How can we best measure whether we have achieved enhanced levels of protection, mitigated a risk, thwarted a threat, or reduced a vulnerability?

Answer: DHS is currently engaged in a study of Measures of Effectiveness, as well as other initiatives to study and implement performance metrics that are meaningful and reflect real progress in securing our borders, critical infrastructure, and the homeland. This effort involves all DHS components, informed by the IAIP's work to assess threat, in the context of our nation's vulnerabilities.

Public Television Datacasting Technologies

Admiral Loy, given your tenure at the Department of Homeland Security, I'm sure you have heard the same clamor from first responders that we in the Senate have heard: they need more spectrum, they need a reliable telecommunications infrastructure. I think it may be useful for the Department to consider the resources that our nation's public television stations can offer as they continue their transition to digital broadcast technology.

Even before the tragedy of 9/11/2001, some public television broadcasters were pioneering "datacasting" systems that use their digital broadcast signal to deliver – wirelessly – large files of electronic information to first responders and others. They can send data in a secure, encrypted format using congestion-free bandwidth to end users that have been equipped with inexpensive DTV tuners. The data can be video, text, graphics, voice – you name it. And it can be sent to first responders in the field as easily as to personnel in an office building.

This is an excellent example of getting the most out of existing infrastructure to solve some of our localities' pressing telecommunications needs. More than half of the nation's public TV stations are already broadcasting in digital, and they are very willing to put some of their valuable bandwidth to public safety use. While this system wouldn't replace two-way radio communications, it does appear to have great potential as a piece of the telecommunications puzzle, and I'd like to see us explore this potential.

Question 2: Would access to secure, uncongested bandwidth at a modest cost be of interest to DHS? Would you be willing to work with Public Television to explore how to capitalize on and benefit from this technology to help solve local, regional and national public safety telecommunications needs?

Answer: The Department of Homeland Security is certainly open to exploring the opportunity of using data-casting technology and its "uncongested bandwith." DHS certainly wants to take advantage of existing capabilities and is willing to work with entities that potentially offer solutions to this critical issue.

QUESTIONS OF SENATOR FRANK R. LAUTENBERG FOR GOVERNMENTAL AFFAIRS COMMITTEE HEARING ON NOMINATION OF ADMIRAL JAMES LOY TO BE DHS DEPUTY SECRETARY
Tuesday, November 18, 2003

Background on Questions One through Five

Over the past two years Washington has moved quickly to legislate, regulate, mandate, spend at the federal level and fund at the local level – though not nearly enough funding for high risk areas. Many federal, state and local agencies as well as the private sector have been busy in their respective worlds supporting technology development and testing technologies in the hope of nailing down the effective solutions.

You are concerned about the coordination required among federal state and local agencies to develop technologies. Take a recent example regarding ocean shipping container security: a month ago, Customs Commissioner Bonner told the industry to start using so-called "smart containers," the Transportation Security Administration (TSA) is said to be planning to put container security requirements in place by the end of the year, and the shipping industry issued a very clear statement that "smart containers" and even electronic seals are not ready for prime time. Meanwhile, Congress has funded $58 million for Operation Safe Commerce (OSC) expressly to test various technologies in international container shipping, a program that you think is invaluable, but the OSC projects have yet to get started. All of which suggests that there may be little coordination in a very crucial area of transportation security.

Question 1: Have the Bureau of Customs and Border Protection and Transportation Security Administration concluded as to what technologies or types of technologies are most effective and will work in a commercial environment to enhance container security?

Answer: Because of the risk that an adversary can defeat any single sensor or device, DHS does not rely on any single technology or inspection process. At our borders, CBP uses a number of technologies in different combinations, including large-scale X-ray and gamma-imaging systems, as well as a variety of portable and handheld technologies, to substantially increase the likelihood that tools of terrorism will be detected. In addition, both through Operation Safe Commerce (OSC) and the Customs Trade Partnership Against Terrorism, and in concert with the Department's Science and Technology division, CBP and TSA are testing the effectiveness and operational feasibility of new technologies that might enhance container supply chain security, to include the security of the containers themselves. OSC demonstration projects are currently underway and initial results are expected by Fall 2004. Specific technologies being examined include electronic seals, global positioning systems (GPS), radio frequency identification systems, and non-intrusive detection systems.

Question 2: What will the Customs Border Protectorate and Transportation Security Administration (TSA) recommend or require of industry to implement in the way of container security measures over the coming year?

Answer: Under the leadership of the Border and Transportation Security Directorate, TSA and CBP are coordinating their efforts and will work with other components of the Department such as the Coast Guard, Science and Technology and the Infrastructure Protection Division of IAIP to enhance the security of containerized cargo entering, exiting, and transiting through the United States. We anticipate that any new standards to be required of industry for containers themselves will be consistent with the International Standards Organization (ISO) high-security mechanical seals for sealing containers, will build on existing programs such as the Customs Trade Partnership Against Terrorism (C-TPAT), the Free and Secure Trade (FAST) program and the Container Security Initiative, and will capitalize on lessons learned through the Operation Safe Commerce program and efforts already underway within the Container Working group.

Question 3: Which agency within the Department of Homeland Security (DHS) has the lead on container security policy including the issuance of Federal standards and other regulatory requirements?

Answer: Development of container security policy, including federal standards and other regulatory requirements, is a responsibility shared between the Border and Transportation Security Directorate's Bureau of Customs and Border Protection and Transportation Security Administration, the United States Coast Guard, the Science and Technology Directorate and the Infrastructure Protection Division of the IAIP Directorate. Although Secretary Ridge has delegated to TSA the lead role in implementing provisions of the Maritime Transportation Security Act (MTSA) requiring development of performance standards for containerized cargo and secure systems of transportation, the delegation also requires that the existing operational expertise of CBP and the USCG be utilized to the maximum extent possible in such development. In specific terms, this means that TSA, CBP, the Coast Guard, under the leadership of Secretary Ridge and Under Secretary Hutchinson, will collaborate with the Department of Transportation to ensure that existing programs that have historically provided security for movement of containerized cargo across our nation's borders, are consistent with and complement efforts to bolster the security of the domestic container supply chain.

Question 4: What is the status of Operation Safe Commerce (OSC)? When will the OSC projects get underway?

Answer: Initial awards have been issued to each of the three Load Centers; the Ports of Seattle/ Tacoma, Los Angeles/Long Beach, and New York/New Jersey. These initial awards allow the Load Centers to access up to 10% of their award funds. Eighteen projects are being funded under those three Load Center awards.

Once the load Centers submit acceptable revised technical proposals and budgets the final cooperative agreement will be issued. This final cooperative agreement will give the Load Centers access to 100% of the cooperative agreement funds.

We anticipate the final awards, to all three Load Centers, will be made in December 2003.

Question 5: Is it the view at the Department of Homeland Security that Operation Safe Commerce will provide important information and experience for determining the best ways to security the international logistics chain?

Answer: Yes, Operation Safe Commerce (OSC) is exploring business processes and technology prototypes to protect commercial shipments from threat of terrorist attack, illegal immigration, and contraband while minimizing the economic impact upon the transportation systems. OSC is currently underway, and, once completed, will provide the public-private partners with best-practice procedures and tested technologies to improve supply chain security.

The Ports of Seattle, Tacoma, Los Angeles, Long Beach, and New York & New Jersey are currently conducting vulnerability assessments of entire international logistics supply chains. They are in the beginning stages of physically testing security devises and procedures on over 1,500 intermodal shipping containers with ports of origin from around the world. These operational tests are being conducted in the real world environment from the containers' point of origin to its final destination.

Projects will include demonstrations to ensure that parties associated with commercial shipping exert reasonable care and due diligence in packing, securing, and manifesting the contents of a shipment of goods in a container. They will also test supply chain security procedures and practices, utilizing enhanced manifest data elements, container sealing, and effective intrusion detection.

Background on Question Six

There is a disconnect between federal security agencies, local law enforcement and other responsible agencies on the sharing of information within the shipping environment. The Customs and Border Directorate is working hard toward full implementation of the ACE computer system but while that will improve information on shipping within DHS it will not make the connection to other actors on the state, regional and local levels who have security responsibility as well. Data is held within government and industry, in a variety of databases, but there is no effective interaction. It seems that even as ACE is being developed work should be undertaken to identify the means--possibly internet based--by which those non-federal agencies can have quick access to shipping information.

Question 6: Do you agree that bridging that information gap is important to there being a quick response capability?

Answer: Yes, and we are working to bridge the information gap between different levels of government. U.S. Customs and Border Protection (CBP) is in the process of implementing the Automated Commercial Environment (ACE). The ACE Secure Data Portal, the foundation of the ACE, was officially adopted by CBP in October. Utilizing a customized computer screen similar to a web site home page, the portal provides a single, centralized on-line access point to connect CBP and the trade community. The portal will also eventually provide on-line access to Participating Government Agencies (PGAs) with trade and border enforcement responsibilities.

Through the development of collaborative tools such as the portal, ACE will provide unprecedented integration of data and communication abilities between CBP, the trade community, and government agencies.

Key to the functioning of ACE and its ability to bridge the information gap between government agencies, is the International Trade Data System (ITDS). The ITDS was chartered in 1995 to promote consolidation and integration of information resources government-wide. The ITDS provides ACE with a format that will ultimately allow the trade community to report data electronically in a standardized manner. The PGAs will then be able to retrieve the information they need through ACE.

Next fall, as ACE is rolled out at the seven busiest land ports, the first PGA will go on-line with ACE, the Federal Motor Carrier Safety Administration of the U.S. Department of Transportation. Other agencies are not far behind. The Animal Plant Health Inspection Service, the Food and Drug Administration, the International Trade Commission, the Maritime Administration, and the U.S. Army Corps of Engineers have begun integration of their operations into ACE/ITDS design and development. The ITDS Board of Directors has also lined up more than 25 federal agencies for ACE/ITDS participation during the next year.

These federal agencies involved in the ITDS effort are sharing information and integrating data with state and local agencies. Many of these initial ACE PGAs already have a strong history of sharing information on a local basis. The ITDS, in conjunction with the ACE infrastructure, has the potential to provide additional integration and sharing of information between federal, state or local government agencies, as well as the trade community, in its dealings with all levels of government.

Question 7: Do you think that the agencies within the Department of Homeland Security should be coordinating on how to best to conduct risk assessments? Is there consistency among the models being used at TSA and elsewhere in DHS?

Answer: Coordination among the agencies within the department is vital. IAIP is working with the various DHS organizations to ensure that risk and vulnerability assessments are conducted using similar methods. When protecting critical infrastructure, it is important to ensure that like methodologies are being used to assess risk and vulnerabilities. IAIP is working with other DHS components to ensure that our assessment of risk as it relates to the nation's interdependent critical infrastructure sectors is informed by agreed upon methodology across government, and that protective and preventive measures are also closely coordinated with all federal, state, local and private partners.

Question 8: Admiral Loy, please describe for me the Administration's view on how best to target federal anti-terrorism assistance to the states and regions where there is reason to believe major public works and systems are targets and at risk of destruction and disruption.

Answer: The Office for Domestic Preparedness and the Information Analysis and Infrastructure Protection Directorate worked closely together to determine funding priorities for the Fiscal Year 2003 and Fiscal Year 2004 Urban Areas Security Initiative. As you know, based on congressional direction in the Department's FY 2003 and FY 2004 appropriations act, this program focuses on high threat, high density urban areas.

Prior to allocating the UASI funds, DHS conducted a thorough and comprehensive review of population and population density, the presence and vulnerability of critical infrastructure of national significance, and credible threat intelligence data from several Federal agencies. Based on this analysis, the Department has determined that 50 urban areas including 30 mass transit systems are eligible funds under the FY 2004 UASI program.

Further, the Department firmly believes that more of the overall funds available to State and local governments need to be distributed using the risk or consequence based formula of population density, presence and vulnerability of critical infrastructure of national significance, and credible threats, while at the same time recognizing that all jurisdictions need a baseline preparedness capability to prevent, respond to and recover from acts of terrorism and natural disasters.

Background on Questions Nine and Ten

Admiral Loy was asked in the pre-hearing questionnaire if he would support the contoured federalization of aviation passenger and baggage screening operations. He was also asked if he would work to maintain TSA's current role in the screening passengers and bagged.

He answered: "First, to my knowledge, a policy decision by the Administration on federalization versus privatization of the screening work force has not been made at this time. However, the Aviation Transportation Security Act does require TSA to enable airports to apply, starting next November 19, for private contractor screeners in place of Federal screeners, and TSA intends to be prepared to ensure effective security with either private contractor screeners or Federal screeners."

Question 9: In your opinion, given your direct role in overseeing security at our airports, do you believe screeners should be federal employees or private sector employees?

Answer: Regardless of the direction taken by the Administration and Congress, I will work to leverage all the tremendous work that TSA has completed and the knowledge that TSA has accumulated since federalization. With or without Federal screeners, TSA will maintain a strong role in screening passengers and baggage. This role may not always be an *operational* one, where TSA actually operates checkpoints as we do today, but it will certainly be, at a minimum, one of regulation and oversight.

Question 10: Do you see an inherent conflict in private companies providing security – a conflict between maintaining adequate security levels and answering to shareholders?

Answer: The Aviation and Transportation Security Act brought tremendous change to the way airport security screening is performed, requiring significant improvements to screener qualifications, training, operational testing and performance for both federal and private security screeners. Provided that robust regulatory oversight is exercised and company compensation is based on the meeting of performance standards and criteria, there should not be an inherent conflict between maintaining adequate security levels and answering to shareholders.

Background on Questions Eleven and Twelve

GAO recently reported that "roughly one – third of terrorist attacks worldwide target transportation systems and transit system." But GAO investigators also found that transit agencies throughout the country are strapped for funds to enhance mass transportation infrastructure. GAO estimated the price to secure of a of the nation's transit systems – public buses, trains, highways – could potentially reach into the billions of dollars

Question 11: In next years funding for the Department, will securing mass transit be a budget priority?

Answer: The Department of Homeland Security anticipates that future Departmental budget requests will provide resources to enhance security in various modes of our transportation system. While current budget planning is pre-decisional to the FY 05 budget request, the Department anticipates building on several current initiatives to provide enhanced security in the transit system. Additionally, Coast Guard's work in implementing the Maritime Transportation Security Act of 2002 will be a complementary initiative as will on-going work of the Science and Technology Directorate to leverage research and development activities for multiple missions. Additional enhancement requests will also provide focused efforts that demonstrate the priority the Administration places on securing the transportation system.

The Department recently announced grant funding through the states to help mass transit agencies across the country enhance the security of their assets and passengers. Allowable uses of funds include installation of physical barricades and area monitoring systems such as video surveillance, motion detectors, thermal/IR imagery and chemical/radiological materials detection systems.

Question 12: You have said that "DHS intends to establish national standards for mass transit? How soon will they be established and will funding be directed toward those systems that fail to meet the standards?

Answer: It is anticipated that as part of the National Transportation System Security Plan, DHS through TSA, working in conjunction with DOT/FTA, will develop a National Mass Transit Security Plan that includes relevant sections on passenger and infrastructure security to address the security of the country's mass transit systems. We are meeting with other modal administrators to complete the NTSSP's draft and put it into broader clearance. We anticipate the completion of the draft phase by the end of the second quarter of 2004.

DHS distributed $115 million in mass transit security grants in calendar year 2003.

Question 13: Admiral Loy, we have had an ongoing gentleman and gentlewoman's disagreement in this committee about the proper funding formula to be used to allocate first responder grant money.

I am curious how you feel about the current grant funding formula, and what changes you will make to it if confirmed.

Answer: DHS believes that funding should be allocated based on threat, but that at the same time, there must also be some base amount of funding provided to ensure that every citizen in the country is adequately protected. DHS accomplishes this balance by administering two complementary programs: The State Homeland Security Grant Program, which utilizes the USA Patriot Act formula; and the Urban Area Security Initiative, which utilizes a risk-based formula taking into account threat, critical infrastructure, and population density. This latter program provides a dedicated funding stream specifically for the nation's higher threat areas. By administering both programs in a consistent and complementary manner, DHS is able to ensure that critical first responder funding is targeted in areas where the threat is highest, while also maintaining a minimum baseline standard in lower-threat areas of the country.

Question for the Record
Submitted by Senator Arlen Specter
for the Nomination of James M. Loy to be
Deputy Secretary of Homeland Security

Admiral Loy, under your leadership, TSA cohosted a conference in March with FAA and NASA to review technologies with potential for countering hostile intentional fire or fuel system assault on commercial aircraft. Several companies and government agencies presented proposals on technologies that could mitigate fuel safety and security concerns. I am advised by one company that participated in the conference that in the eight months that have passed, there has been no concerted effort by TSA or the other agencies to begin evaluating these technologies. Congress has appropriated a considerable amount of funds for FY2004 for research and development programs within the Department of Homeland Security, and I would appreciate your providing the Committee with detailed information that will give us a sense of how your agency will build on the results of the March, 2003 conference and evaluate these technologies for future use in protecting the general public.

ANSWER:
On March 11-12 2003, NASA, FAA and TSA organized a workshop on "Aircraft Fire/Fuel Safety and Security." The primary objective of the workshop was to provide data for NASA and FAA (not TSA) aircraft fire and fuel safety managers with which they could, in part, determine the most appropriate use of FY04 resources in fire/fuel safety research that has potential to enhance aircraft survivability. The TSA's role has been clearly focused towards providing NASA with requirements and priorities, from a security perspective, to enhance the performance of fire and fuel systems in the event of terrorist attack.

The 7-member panel at the workshop was chaired by a representative from the Department of Defense, TSA had a representative on this panel. After reviewing the presentations, the panelists evaluated the technologies across several criteria including technology readiness level, riskiness of development, and threat coverage (i.e., how many threats would the solution protect against). This information was provided to the workshop participants in a final report.

In the area of aircraft fuel/fire research, the FAA, DOD, and NASA have well regarded, established programs. The TSA's strategy has been to share its requirements with these organizations in an effort to coordinate the government's investment in fuel and fire system protection technology in a manner that benefit both safety and security. It is the subject matter experts within the FAA, NASA, and DOD who ultimately will evaluate and recommend technologies for the potential to enhance aircraft survivability in this area.

04-0301

Deputy Secretary
U.S. Department of Homeland Security
Washington, DC 20528

February 23, 2004

The Honorable Susan Collins
Chairman
Committee on Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Collins:

This letter is to notify you of a factual error contained in my response to the committee's pre-hearing questionnaire for my nomination to the position of Deputy Secretary of the Department of Homeland Security. The error is contained in my response to question 63, which seeks information about the Transportation Security Administration's (TSA) role in the exchange of passenger data from JetBlue Airways to Torch Concepts.

At the time I responded to your questionnaire, we were relying on the memory of a TSA employee who had dealt with this matter in the May/June 2002 time frame. At about the same time the response was prepared, in order to respond to a series of detailed questions from Senator Patrick Leahy, TSA began to search its files for written material related to the JetBlue matter. As a result of this search, we uncovered new information that will be reflected in the response to Senator Leahy's questions. To ensure that my responses to the prehearing questions are complete and accurate, I respectfully request that I be permitted to amend my response to this question.

I am enclosing my revised answer to this question along with a copy of my original responses. I would be happy to answer any further questions you may have on this matter.

Sincerely Yours,

J.M. Loy, ADM
Deputy Secretary

04-0301

Original Answer

U.S. Senate Committee on Governmental Affairs
Pre-hearing Questionnaire
For the Nomination of James M. Loy to be
Deputy Secretary of the Department of Homeland Security

63. The recent disclosure that over a million JetBlue passengers had their personal information disclosed to a U.S. Army data-mining contractor has raised further concerns about programs like CAPPS II. Although the Department has repeatedly claimed that it will not use data collected for screening purposes to examine credit histories and similar information in commercial databases, reports are that Torch Concepts may have done precisely that in its research for the Army. Were the reported contacts between TSA and the Army contractor, Torch Concepts, related in any way to CAPPS II? Has Torch Concepts done any work for TSA related to CAPPS II?

Answer: Torch Concepts has not performed any work for TSA related to the development or operation of CAPPS II.

The extent of TSA's contacts with the Army contractor, Torch Concepts, were limited to a single briefing TSA attended in May or June of 2002, which was set up and attended by DOD. At the time, TSA understood Torch Concepts to be working on an application that would conduct a risk-evaluation of commercial airline passengers arriving in the area of a military base to determine the level of risk that was posed to the base at any given time. TSA was interested in learning more about the Torch Concepts approach because, at the time, TSA was actively considering various ideas for the ultimate concept for CAPPS II. The briefing on the Torch Concepts application gave TSA the opportunity to learn about a sister agency's potential approach to aviation-passenger risk evaluation.

At the briefing, DOD asked for TSA's assistance in obtaining the PNR data that Torch Concepts needed to provide a proof of concept for its application. TSA provided that assistance only in the form of an introduction for DOD to JetBlue Airlines, after JetBlue indicated an interest in potentially supporting DOD's efforts in this area. TSA did not facilitate, negotiate, or otherwise participate in any arrangement DOD and JetBlue ultimately reached regarding the provision of PNR data for the Torch Concepts project. TSA's limited efforts in this area were not related to CAPPS II.

04-0301

Amended Answer

U.S. Senate Committee on Governmental Affairs
Pre-hearing Questionnaire
For the Nomination of James M. Loy to be
Deputy Secretary of the Department of Homeland Security

63. The recent disclosure that over a million JetBlue passengers had their personal information disclosed to a U.S. Army data-mining contractor has raised further concerns about programs like CAPPS II. Although the Department has repeatedly claimed that it will not use data collected for screening purposes to examine credit histories and similar information in commercial databases, reports are that Torch Concepts may have done precisely that in its research for the Army. Were the reported contacts between TSA and the Army contractor, Torch Concepts, related in any way to CAPPS II? Has Torch Concepts done any work for TSA related to CAPPS II?

Answer: Torch Concepts has not performed any work for TSA related to the development of CAPPS II.

In the May/June 2002 timeframe, DOD requested TSA's assistance in obtaining airline passenger data for use by Torch Concepts. TSA attended a briefing by Torch Concepts which was set up and attended by DOD. At the time, TSA understood Torch Concepts to be working on an application that would conduct a risk-evaluation of commercial airline passengers arriving in the area of a military base to determine the level of risk that was posed to the base at any given time. TSA was interested in learning more about the Torch Concepts approach because, at the time, TSA was actively considering various ideas for the ultimate concept for CAPPS II. The briefing on the Torch Concepts application gave TSA the opportunity to learn about a sister agency's potential approach to aviation-passenger risk evaluation.

At the briefing, DOD asked for TSA's assistance in obtaining the PNR data that Torch Concepts needed to provide a proof of concept for its application. In a July 30, 2002 memorandum, TSA requested that JetBlue provide archived passenger data to the DOD. A copy of that memorandum and the cover email is attached. TSA's limited efforts in this area were not related to CAPPS II. Any value accruing to TSA's work in aviation security would have been lessons learned from DOD's project.

MEMORANDUM

DATE: July 30, 2002

TO: Robert DeFrancesco
Director, Corporate Security
Jet Blue Airlines [718-286-4096]

FROM: Mark T. Torbeck
CAPPS II Office

SUBJECT: **Request for PNR Data for a Department of Defense (DoD) Proof of Concept**

cc: Stephen L. Cohn
Office of the Assistant Secretary of the Army
(Acquisition, Logistics and Technology)
International Programs Manager
703-601-1556

Roy Nichols - Chair of company - Acumen
Torch Concepts
256-885-0168

As discussed, the Department of Defense (DoD) is currently involved in a Proof of Concept program for the purposes of improving military base security. DoD engaged the Transportation Security Administration (TSA) to assist in the securing of passenger name record (PNR) data to help meet this proof of concept initiative.

For this stated reason, TSA is requesting the use of archived PNR data belonging Jet Blue. We are requesting that Axiom, a contractor who provides PNR data parsing services to Jet Blue, provide this PNR data to the DoD contractor, Torch Concepts. Any non-disclosure agreements that need to be executed can be exchanged directly between the parties with copies provided to both DoD and TSA.

Torbeck, Mark

From:	Torbeck, Mark
Sent:	Wednesday, July 31, 2002 10:01 AM
To:	'Bob.DeFrancesco@jetblue.com'
Cc:	'mcholsr@torchconcepts.com'; 'Stephen.Cohn@saalt.army.mil'
Subject:	Concept of Operations - PNR Data usage

Bob:
Thank you so much for your quick response and participation in support of this critical project involving base security. We at the TSA are working with DOD to support this effort. In conjunction with this effort, attached plz find the letter of request [which includes phone numbers] regarding PNR data being provided to Torch Concepts for this proof of concept.

If you have any question, plz do not hesitate to call. DOD is looking to kick this project off ASAP for all the obvious reasons, so anything you can do to help expedite the movement of the data between Axiom and Torch would be greatly appreciated.

Mark

B - 919-485-0770
C - 919-270-4964

DOD
ent with Jet Bl