DISRUPTING TERRORIST TRAVEL: SAFEGUARDING AMERICA'S BORDERS THROUGH INFORMATION SHARING

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY

AND THE

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERRORISM

OF THE

SELECT COMMITTEE ON HOMELAND SECURITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

SEPTEMBER 30, 2004

Serial No. 108–60

Printed for the use of the Select Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

25–777 PDF WASHINGTON : 2006

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

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
DON YOUNG, Alaska
F. JAMES SENSENBRENNER, JR., Wisconsin
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
JOE BARTON, Texas
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PORTER J. GOSS, Florida
DAVE CAMP, Michigan
LINCOLN DIAZ-BALART, Florida
BOB GOODLATTE, Virginia
ERNEST J. ISTOOK, JR., Oklahoma
PETER T. KING, New York
JOHN LINDER, Georgia
JOHN B. SHADEGG, Arizona
MARK E. SOUDER, Indiana
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
KAY GRANGER, Texas
PETE SESSIONS, Texas
JOHN E. SWEENEY, New York

JIM TURNER, Texas, *Ranking Member*
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
KAREN MCCARTHY, Missouri
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
BEN CHANDLER, Kentucky

JOHN GANNON, *Chief of Staff*
STEPHEN DEVINE, *Deputy Staff Director and General Counsel*
THOMAS DILENGE, *Chief Counsel and Policy Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MARK T. MAGEE, *Democrat Deputy Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY

DAVE CAMP, Michigan, *Chairman*

KAY GRANGER, Texas,
JENNIFER DUNN, Washington
DON YOUNG, Alaska
DUNCAN HUNTER, California
LAMAR SMITH, Texas
LINCOLN DIAZ-BALART, Florida
ROBERT W. GOODLATTE, Virginia
ERNEST ISTOOK, Oklahoma
JOHN SHADEGG, Arizona
MARK SOUDER, Indiana
JOHN SWEENEY, New York
CHRISTOPHER COX, California, *Ex Officio*

LORETTA SANCHEZ, California, *Ranking Member*
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
KENDRICK B. MEEK, Florida
JIM TURNER, TEXAS, *Ex Officio*

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

JIM GIBBONS, Nevada, *Chairman*

JOHN SWEENEY, New York
JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
HAROLD ROGERS, Kentucky
CHRISTOPHER SHAYS, Connecticut
LAMAR SMITH, Texas
PORTER GOSS, Florida
PETER KING, New York
JOHN LINDER, Georgia
JOHN SHADEGG, Arizona
MAC THORNBERRY, Texas
CHRISTOPHER COX, California, *Ex Officio*

KAREN MCCARTHY, Missouri, *Ranking Member*
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
JIM TURNER, TEXAS, *Ex Officio*

CONTENTS

Page

STATEMENTS

The Honorable Dave Camp, a Representative in Congress From the State of Michigan, and Chairman, Subcommittee on Infrastructure and Border Security:
Oral Statement 1
Prepared Statement 4
The Honorable Loretta Sanchez, a Representative in Congress From the State of California, and Subcommittee on Infrastructure and Border Security 20
The Honorable Jim Gibbons, a Representative in Congress From the State of Nevada, and Chairman, Subcommittee on Intelligence and Counterterrorism 4
The Honorable Karen McCarthy, a Representative in Congress From the State of Missouri, and Ranking Member, Subcommittee on Intelligence and Counterterrorism 24
The Honorable Christopher Cox, a Representative in Congress From the State of California, and Chairman, Select Committee on Homeland Security: Prepared Statement 2
The Honorable Jim Turner, a Representative in Congress From the State of Texas, and Ranking Member, Select Committee on Homeland Security 36
The Honorable Robert E. Andrews, a Representative in Congress From the State of New Jersey 26
The Norman D. Dicks, a Representative in Congress From the State of Washington 42
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island 34
The Honorable Nita M. Lowey, a Representative in Congress From the State of New York 31
The Honorable Bill Pascrell, Jr., a Representative in Congress From the State of North Carolina 28

WITNESSES

Lieutenant General Patrick Hughes, Assistant Secretary for Information Analysis, Department of Homeland Security:
Oral Statement 5
Prepared Statement 6
The Honorable C. Stewart Verdery, Jr., Assistant Secretary, Border and Transportation Security Policy and Planning, Department of Homeland Security:
Oral Statement 9
Prepared Statement 11
Professor Lawrence M. Wein, Graduate School of Business, Stanford University:
Oral Statement 38
Prepared Statement 40

FOR THE RECORD

The Honorable C. Stewart Verdery, Jr. and Lieutenant General Partrick Hughes Responses:
Questions from the Honorable Christopher Cox 49
Questions from the Honorable Dave Camp and the Honorable Jim Gibbons . 52

Page

Professor Lawrence M. Wein Responses to Questions:
Questions from the Honorable Dave Camp and Chairman Gibbons 68

DISRUPTING TERRORIST TRAVEL: SAFEGUARDING AMERICA'S BORDERS THROUGH INFORMATION SHARING

Thursday, September 30, 2004

HOUSE OF REPRESENTATIVES,
SELECT COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INFRASTRUCTURE
AND BORDER SECURITY,
AND THE
SUBCOMMITTEE ON INTELLIGENCE
AND COUNTERTERRORISM,
Washington, DC.

The subcommittees met, pursuant to call, at 1:05 p.m., in Room 210, Cannon House Office Building, Hon. Dave Camp [chairman of the Subcommittee on Infrastructure and Border Security] Presiding.

Present from Subcommittee on Infrastructure and Border Security: Representatives Camp, Dunn, Sanchez, Dicks and Pascrell.

Present from Subcommittee on Intelligence and Counterterrorism: Gibbons, Dunn, McCarthy, Langevin, Dicks, Lowey and Andrews.

Mr. CAMP. The joint hearing of the Subcommittee on Infrastructure and Border Security and the Subcommittee on Intelligence and Counterterrorism will come to order. The subcommittees are meeting jointly today to hear testimony on the Department of Homeland Security's efforts regarding terrorists' disruption of travel. The purpose of this hearing is to look at the recommendations made by the 9/11 Commission report and examine DHS's efforts to obtain, analyze and disseminate terrorist travel information.

On the first panel we have General Patrick Hughes, who is the Assistant Secretary for Information Analysis, and Assistant Secretary Stewart Verdery from the Border and Transportation Security Policy Office. And on the second panel we will hear from Professor Lawrence Wein from Stanford University, who will provide an overview of research he has done regarding the US-VISIT program. And I would like to officially welcome all of our witnesses.

I ask unanimous consent that Member opening statements be included in the hearing record, and encourage members of both subcommittees to submit their opening statements for the record.

[The information follows:]

PREPARED OPENING STATEMENT OF THE HONORABLE CHRISTOPHER COX, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND CHAIRMAN, SELECT COMMITTEE ON HOMELAND SECURITY

Let me begin by commending Chairman Camp and Chairman Gibbons for working collaboratively to address the critical issue of terrorist travel and information sharing. I also would like to welcome and thank Assistant Secretary Hughes and Assistant Secretary Verdery for appearing before the panel today.

Over the past 18 months, DHS has implemented several reforms to strengthen our Nation's borders and improve information sharing—from enhancing the National Targeting Center to strengthening relationships with state and local law enforcement. Further, President Bush continues to provide strong leadership to strengthen our collective security, with the creation of the Terrorist Screening Center (TSC) and the Terrorist Threat Integration Center (TTIC), and now the National Counterterrorism Center. Although these reforms have made us safer, there is still more work to be done. Currently, Congress is considering a wide range of legislative proposals and will soon deliver a set of reforms designed to further facilitate information sharing between our intelligence and homeland security agencies, and to strengthen our security here at home.

The 9/11 Commission report helped to energize the current debate in these chambers about homeland security and information sharing within our intelligence communities. The Commission's report focused significant attention on the issue now commonly referred to as "terrorist travel." The 9/11 Commission Report urges us to address the issue of terrorist travel with the same vigor and focus that we are brining to terrorist financing.

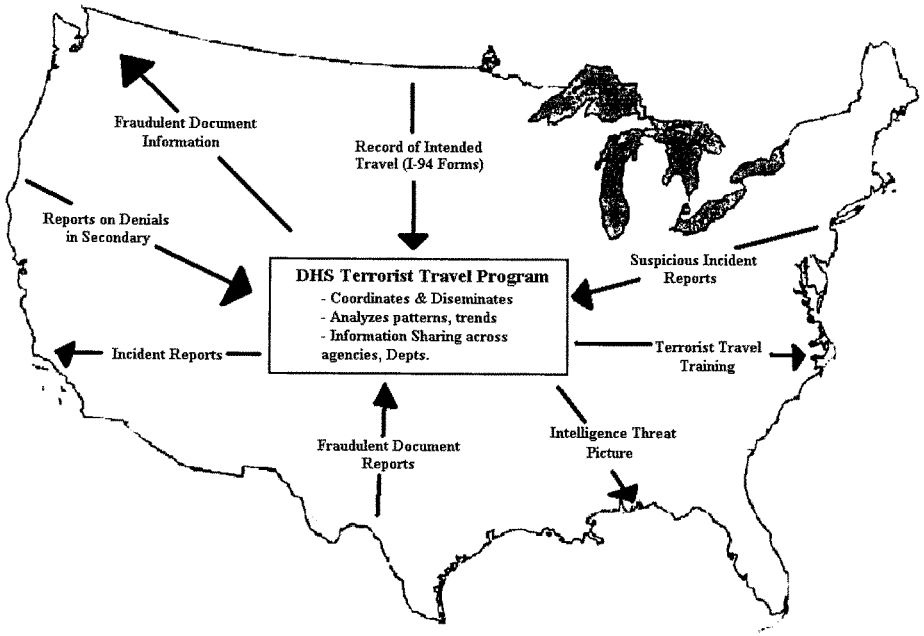
I wholeheartedly agree and am glad to see that Speaker Hastert's 9/11 Commission recommendations implementation bill incorporates many significant provisions relating to terrorist travel, some of which were proposed by this Committee.

While limiting access to money hinders terrorists' ability to carry out a mission, combating terrorist travel, especially into the United States, will significantly disrupt our enemy's ability to move operatives into position to launch an attack. Today, we will examine how DHS currently is organized to address this critical issue, and discuss how the Department should move towards further implementation of the Commission's recommendation in this area.

In discussing the issue of terrorist travel, the Commission stated, "For terrorists, travel documents are as important as weapons. Terrorist must travel clandestinely to meet, train, plan, case targets, and gain access to attack. To [terrorists], international travel presents great danger, because they must surface to pass through regulated channels, present themselves to border security officials, or attempt to circumvent inspection points. In their travels, terrorists use evasive methods, such as altered and counterfeit passports and visas, specific travel methods and routes, liaisons with corrupt government officials, human smuggling networks, supportive travel agencies, and immigration and identity fraud."

Combating terrorist travel will require a multi-faceted approach that will reach across several DHS components and agencies. Potential terrorists may interact with the U.S. Government at an embassy or consular office overseas, a Border Patrol agent if they cross between ports-of-entry or are stopped at an interior checkpoint, a U.S. Customs and Border Protection inspector at our land and air ports-of-entry, and the U.S. Coast Guard on our waters and at our sea ports-of-entry.

An Integrated Terrorist Travel Strategy



This chart demonstrates the various pieces of information and multiple agencies involved in combating terrorist travel. Integrating this information and analyzing potential trends is critical to a successful effort in targeting terrorist travel. These known trends, patterns, tactics, and practices need to be coupled with any fraudulent document information and merged into a complete threat picture. Sharing this information overseas with consular agents and with front line agents at borders and ports of entry across the United States is critical and will ensure a unified U.S. Government strategy in combating terrorist travel.

Every encounter presents an opportunity for our front-line DHS personnel to disrupt terrorist travel. The ever-changing and developing intelligence and information related to terrorist travel techniques, documents, and trends needs to be effectively incorporated into the daily activities of our front-line DHS personnel, and we will discuss today how to make that happen as effectively as possible.

In addition, international efforts also are required to effectively combat terrorist travel, and will involve our DHS personnel located overseas, working hand in hand with their State Department counterparts. If a terrorist's ability to travel is limited before reaching our borders, our homeland security will be strengthened and we will move closer to winning the War on Terrorism.

We need to continue to tear down the walls and improve sharing of information in order to make continued progress in homeland security. Success in this struggle depends upon good information getting to the right people at the right time.

I look forward to your testimony this afternoon, and thank you for your appearance today.

Mr. CAMP. And because this is a joint hearing, Members will be recognized based on order of appearance. And having said that, I will submit my opening statement for the record.

[The information follows:]

PREPARED OPENING STATEMENT OF THE HONORABLE DAVE CAMP, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN, AND CHAIRMAN, SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY

Disrupting terrorists in their efforts to enter into and freely travel within the United States is a critical part of fighting the War on Terrorism. The 9/11 Commission Report highlighted the flaws in U.S border and immigration laws that the 9/11 hijackers exploited. Many of these gaps have been addressed since September 11th, yet the Commission stressed that terrorist travel must remain a specific focus of security efforts.

I hope to stress with this hearing that DHS must continue to develop and expand its ability to analyze terrorist techniques, patterns, indicators, and trends to enable front line personnel to identify, intercept, and disrupt terrorist seeking to travel to the United States.

One thing that is very apparent is that DHS has a very wide range of resources and capabilities to disrupt terrorist travel. However, it is unclear to me how well all of these resources are utilized and coordinated. There is the National Targeting Center, the Fraudulent Documents Lab, Benefit Fraud Units, various BTS and Coast Guard intelligence offices, and Information Analysis Division. And that's just to name a few. With resources spread across the department, one of the concerns I have is making sure that there is a dedicated focus to ensure that terrorist travel detection remains a priority and that there is Department-wide coordination effort.

There is no doubt that combating terrorist travel will require a multi-faceted approach across all DHS components and several other Federal agencies. Potential terrorists may interact with the U.S. Government at an embassy or consular office overseas, a border and immigration inspector, or a TSA screener as they seek to travel within the U.S.

Each of these encounters presents an opportunity to detect terrorist travel. In addition, numerous pieces of information are used throughout this process, including visas, passports, travel plans, and intelligence reports. Given these various pieces of information and encounters with potential terrorists, this information needs to be integrated across the Federal government to create a current threat picture that can be used to identify and stop terrorist travel.

I look forward to hearing from our witnesses today as they seek to address these very important issues.

Mr. CAMP. And at this time I would recognize Mr. Gibbons. Chairman of the Intelligence and Counterterrorism Subcommittee is now recognized for any opening statement he may have.

Mr. GIBBONS. Thank you very much, Chairman Camp. And to our guests today, welcome. General Hughes, it is great to see you back before us. And, Assistant Secretary Verdery, thanks very much for your presence here as well today. It is an important hearing we are going to have today and I know that your testimony is very valuable, and I, like Chairman Camp, am going to follow his

lead and put my opening statement into the record so that we can move along quickly and expeditiously so that we don't take more of your time.

I know that you are both facing immense challenges right now, and it is an exceedingly important job, and we look forward to hearing your testimony today.

And with that, Mr. Chairman, I will submit my testimony for the record.

Mr. CAMP. All right. I think at this point—are there any other opening statements?

All right. I think at this point we will go to our witnesses, and I again like to thank them for being here. General Hughes, we will begin with you. We have received your written testimony, and we will ask that you briefly summarize in 5 minutes your statement. Thank you.

STATEMENT OF LIEUTENANT GENERAL PATRICK HUGHES, ASSISTANT SECRETARY, INFORMATION ANALYSIS, DEPARTMENT OF HOMELAND SECURITY

General HUGHES. Thank you very much, and good day, Chairman Camp and Chairman Gibbons and distinguished members of the committee, joint committees I guess.

As you know, the Department of Homeland Security was envisioned, formed and is now in operation. President Bush's decision to establish the Department has enabled us to unify our diverse resources into one team to prevent terrorism in the whole land, to ready ourselves against our enemy, and to ensure the highest level of protection for our country and the citizens we serve.

Through the Homeland Security Act of 2002, among other things, we are charged with integrating relevant information, intelligence analysis and vulnerability assessments to identify threats, to inform preventive priorities and to support protective measures. We are doing this in partnership primarily with Federal partners and State and local governments, agencies, and other organizations that we find at the State and below level, and with our partners in the private sector.

The Office of Information Analysis, which I represent, is the heart of intelligence at the Department of Homeland Security. It is responsible for accessing and analyzing the entire array of intelligence related to threats against the homeland and making that information useful to our Federal partners, first responders, and anyone in the United States who can use that information and has the right to receive it. IA provides a full range of intelligence support to the Secretary and DHS leadership and to all of our components. Additionally, IA assures that the best intelligence information available informs the administration of the Homeland Security Advisory System.

In order to perform these duties, we must receive intelligence from a number of sources, including not only the United States Intelligence Community and our State, local, territorial, tribal and private sector partners, but also from Department of Homeland Security entities with intelligence capabilities. The large amount of information we coordinate includes reporting from the United States Secret Service, the United States Coast Guard; the Border

and Transportation Security Directorate; Immigration and Customs Enforcement, including the Federal Protective Service and the Federal Air Marshal Service; Customs and Border Protection; the Transportation Security Administration; the Office of Citizenship and Immigration Services; and the Federal Emergency Management Agency; 180,000 plus persons on the ground throughout the country acting as eyes and ears, enforcers, and workers, and policymakers in some cases in order to protect the country.

We represent a primary element of the United States Intelligence Community, a powerful source of information and a powerful capability in order to use the information we have to protect our citizens. We have a sense of purpose, and we have embarked on what has likely never been done before with regard to information fusion: to fully understand the threat and the conditions that make that information useful at a utilitarian level for such a broad range of officials from city mayors to Border Patrol agents, to airport screeners, to critical infrastructure operators, to the cop on the beat.

This concludes my oral statement. I would be happy to answer any questions you have today, and I am looking forward to our interaction. Thank you.

Mr. CAMP. Thank you very much.

[The statement of General Hughes follows:]

PREPARED STATEMENT OF PATRICK M. HUGHES

Good morning Chairman Camp, Chairman Gibbons, and distinguished members of the Committee. I am privileged to appear before you today to discuss information sharing and collaboration, and the role of the Office of Information Analysis (IA), within the Information Analysis and Infrastructure Protection Directorate (IAIP) of the Department of Homeland Security (DHS).

In the aftermath of 9/11, the Department of Homeland Security was envisioned, formed, and is now in operation. Standing up the Department, the largest reorganization of government in fifty years, has been a great undertaking. Many employees of DHS have assumed new responsibilities, and all have put in long hours to ensure that while our strategies may change to meet the terrorist threat, our course as a nation will remain constant. President Bush's decision to establish the Department has enabled us to unify our diverse resources into one team, to ready ourselves against our enemy, and to ensure the highest level of protection for our country and the citizens we serve.

Through the Homeland Security Act of 2002, IAIP, and consequently IA, is charged with "integrating relevant information, intelligence analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) to identify protective priorities and support protective measures by the Department, by other executive agencies, by State and local government personnel, agencies, and authorities, by the private sector, and by other entities." In addition, Section 892 of the Homeland Security Act and Executive Order 13311 establish the Secretary of Homeland Security as responsible for information sharing across the Federal government and with State, Tribal, and local government, as well as private sector security responsible for protecting the nations critical infrastructure. The Secretary has delegated this to the Under Secretary for IAIP.

IA is the heart of the intelligence effort at DHS. It is responsible for accessing and analyzing the entire array of intelligence relating to threats against the homeland, operational reporting from across DHS and State and local law enforcement, and assimilating disparate operational and intelligence information, making that information useful to federal partners, first responders, State, territorial, tribal, local, and major city governments, and the private sector. IA provides the full-range of intelligence support to the Secretary, DHS leadership, the Undersecretary for IAIP, and DHS components. Additionally, IA ensures that the best intelligence available informs the administration of the Homeland Security Advisory System.

In order to perform these duties, IA must receive intelligence from a number of sources, including the United States Intelligence Community (IC), particularly the Federal Bureau of Investigation- the primary interface with law enforcement entities around the country, and our afore mentioned State, territorial, tribal, local and private sector partners, but also from all DHS entities with intelligence capabilities as well as DHS operational entities. The large amount of information IA coordinates includes reporting from the United States Secret Service (USSS), the United States Coast Guard (USCG), the Border and Transportation Security Directorate (BTS), Immigration and Customs Enforcement (ICE) including the Federal Protective Service (FPS) and the Federal Air Marshal Service (FAMS), Customs and Border Protection (CBP), the Transportation Security Administration (TSA), the U.S. Citizenship and Immigration Services (CIS), and the Federal Emergency Management Agency (FEMA). In addition, IA interfaces with our colleagues in the Infrastructure Protection (IP) Office of the IAIP Directorate to achieve one the cornerstones of the Department of Homeland Security, to deliver threat-informed vulnerability and risk assessments regarding our critical infrastructure, to our constituents and customers—notably the private sector that holds most of our nation's critical national infrastructure. We are an integral part of the Homeland Security Operations Center (HSOC) effort to monitor and communicate on all matters of homeland security interest 24X7. We also relate directly to the Integrated Staff element of DHS, the operations directorate that is responsible for planning and developing operations concepts and orders to DHS components and to our partner organizations. We attend all IC and White House collaboration and coordination meetings, including many that are accomplished by secure video teleconference. Our involvement in information sharing and collaboration includes all of this and more.

Information sharing and collaboration is not a one-way street. In addition to receiving information from these entities, IA delivers the intelligence it coordinates to our partners as appropriate. This requires IA to share information and collaborate at all levels, from the Federal Government and IC members to local officials and DHS entities that in turn provide threat information to their associates on the front line. DHS component organizations not only provide support to IA and to their associates, they also serve as a conduit through which relevant information can pass to DHS and the rest of government and information and warnings can be shared with stakeholders within their areas of responsibility—thereby increasing the practical benefits derived from intelligence analysis.

IA analysts have access to the most classified and highly sensitive national intelligence from the Terrorist Threat Integration Center (TTIC) (whose responsibilities will eventually be assumed by the National Counterterrorism Center—NCTC), the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the Department of State (DoS), and other national-level agencies regarding international and domestic terrorist threats. This information is received formally through IA analysts' connections to the Joint Worldwide Intelligence Communications Systems (JWICS), TTIC Online, the IA Automated Message Handling System (AMHS), the Homeland Security Information Network (HSIN), and a variety of other formal and informal (i.e., analyst-to-analyst) mechanisms that contain such intelligence. This information from other agencies is augmented by our own internal reporting from DHS components.

From Border and Transportation Security (BTS) reports regarding individuals of interest trying to enter the United States illegally, to USCG reports regarding suspicious activity near critical infrastructure points, intelligence from DHS components that IA analyzes provides invaluable perspective and insight for the entire Federal Government. Such reports are provided to IA through the same methods the IC uses- the physical presence of DHS component liaison officers within both IA and the Homeland Security Operations Center (HSOC) and communication between analysts and leadership. In fact, the presence of representatives of 26 separate Federal and local representatives within HSOC provides a perspective and collaboration capability which is very valuable. Additionally, coordination within DHS is aided by regular meetings of the intelligence chiefs of each entity, lead by the Assistant Secretary for Information Analysis (ASIA).

Information moves into and out of IA in the form of a number of different documents. Many are familiar with the Homeland Security warning products that communicate valuable threat information to such varied audiences as the public, first responders, and infrastructure owners. Homeland Security Information Bulletins provide a means to communicate information of interest to the nation's critical infrastructures that does not meet the timeliness, specifics, or significant thresholds of warning messages. They are designed to provide updates on the training, tactics, or strategies of terrorists. Similarly, Homeland Security Threat Advisories identify

a threat targeting critical national networks or key infrastructure assets and provide a means for DHS to communicate threat information to all DHS customers ranging from the IC to the general public. This information stream is augmented by other products, such as Special Assessments and Studies, Homeland Security Intelligence Articles, and Red Cell reports, which offer alternative or conceptual analysis. Additionally, Homeland Security Information Messages (HSIMs) are a valuable tool used to expeditiously communicate newly acquired, uncorroborated threat information to U.S. government agencies, state and local Homeland Security Advisors, and the private and public sectors. The HSIM contains a preliminary analysis of threat information received by DHS from the intelligence community, law enforcement community, private or public sector and have information that has not been fully evaluated.

In addition to these products, IA employs a variety of reporting mechanisms to communicate with both IC members and the intelligence offices of DHS operational components. Intelligence goes to DHS component entities and the IC primarily through DHS Intelligence Information Reports (IIRs) and Homeland Security Intelligence Reports (HSIRs). The IIR quickly releases select raw intelligence reporting from DHS components to the IC, Federal Law Enforcement, and others as appropriate in a unified and recognizable format via the Automated Message Handling System (AMHS). Similarly, a HSIR provides DHS operational elements a vehicle to report case and potential terrorist information to DHS headquarters. It is a final report, containing a compilation of information where some processing or analysis has occurred and should stand alone as a semi-finished product. Lastly, information is shared and coordination occurs through the IA Executive Morning Brief (IAEMB), which is shared at the daily morning intelligence update and through the twice-daily Secure Video Teleconference (SVTC), as well as through direct analyst-to-analyst and leadership communication.

It is IA's singular focus on the protection of the American homeland against terrorist attack that is unique among its IC partners. This focus provides invaluable information and assistance not only to State, territorial, tribal, local, and private sector officials that receive accumulated threat information, but also to DHS components that use the information, trends, and indicators to inform and prepare operators and decision makers on the front line. The relationship IA has with the HSOC, BTS and other DHS entities translates into continuous information sharing and collaboration that provides a unique threat picture to those who are vital to protecting the homeland.

The Department of Homeland Security is a prime example of how changes have been made within the Intelligence Community, the counterterrorism community, and the law enforcement community to work more cohesively as well as more collaboratively, to assure information is shared as fully and completely as possible. This represents a dramatic change from conditions as they existed before September 11th, 2001. DHS plays a central role in the counter-terrorism and homeland security effort as we continue the work of communicating intelligence and information to our partners in the federal government as well as with the State, territorial, tribal, local, and private sector officials charged with protecting the people and infrastructure of this country.

Building up IA, increasing our information capabilities, and coordinating intelligence information sharing and collaboration across the entire federal government are monumental tasks. We have accomplished much in a short period of time and we continue to press forward to strengthen our capabilities and our ability to support the overall DHS mission set. In order to better facilitate this effort the Department of Homeland Security has formed the DHS Information Sharing and Collaboration (ISC) Program, appointed a Director, and formed a staff including representation from all internal components. We are a participating member of the larger national effort to improve and enhance information sharing and collaboration and to integrate ISC concepts and capabilities into the changing intelligence community (IC) environment under the various transformation efforts brought forth by the 9–11 Commission and by earlier and subsequent Administration and Congressional action. The DHS ISC Program has already begun the work of assessing the "here and now," of envisioning and forming a future Information Sharing Architecture, and is engaged in building the business plan which will guide and govern efforts to construct the appropriate enterprise architecture to empower full and complete sharing throughout the entire Homeland Security environment. One of the major DHS programs the ISC Program now collaborates on is the Homeland Security Information Network (HSIN)–an overarching network for the Department to provide information exchange and real time collaboration between federal, state, local, tribal, and major city authorities. Using this network, federal, state, and urban area homeland security advisors are able to communicate with each other and with DHS. As a direct

result of ISC Program efforts to cooperate and work jointly with other Federal partners, DHS and the Department of Justice (DOJ)/FBI have established the first ever capability to share information between the HSIN/Joint Regional Information Exchange System (HSIN/JRIES), the Regional Information Sharing System (RISSNet), Law Enforcement Online (LEO), and will soon be joined by the Criminal Information Sharing Alliance Network (CISANet). Through this technology demonstration project, Sensitive But Unclassified products of each department and network are posted to other networks thereby allowing users on any of the systems to see and use the products from the other organizations.

Many of the efforts we are undertaking are technical in nature, but the primary effort is not merely technical but rather one of changing policy and procedure to motivate and empower necessary technical change in order to achieve our goals of functional interoperability and information transparency in order to accomplish the information sharing and collaboration mission. However, it must be noted that intelligence analytic tools such as link and nodal analysis tools, very dynamic search engines tailored for the intelligence data base environment, analytic workstations configured to empower the analysts in their work, and numerous other technical aids and capabilities. . .are key to our information sharing and collaboration success.

We have accomplished much at DHS and in IA since our inception and we are on course with our partners and colleagues to continue to achieve. I firmly believe the American people are more secure and better prepared than before September 11, 2001 directly because of the advent of the Department of Homeland Security. We are fully connected to the U.S. Intelligence Community and well informed. We are more fully integrated into the workings of the domestic security structure. We are connected with law enforcement. We have working analysts poring over the detail of intelligence and law enforcement reporting to discover the hidden patterns and concealed threads of terrorist activity and the manifestation of other threats to America from crime with national security implications and from other disasters and threatening conditions that come our way. We have a sense of purpose and we have embarked on what has likely never been done before with regard to information fusion. . .to fully understand the threat and the conditions to make that information useful at a utilitarian level for a broad range of officials from city mayors to border patrol agents to airport screeners to critical infrastructure operators to the cop on the beat.

Chairman Camp, Chairman Gibbons, and Members of the Committee, this concludes my prepared statement. I would be happy to answer any questions you may have at this time.

Mr. CAMP. Mr. Verdery, you have 5 minutes. We have your written statement, and if you could summarize it, that would be helpful.

STATEMENT OF C. STEWART VERDERY, JR., ASSISTANT SECRETARY, BORDER AND TRANSPORTATION SECURITY POLICY AND PLANNING, DEPARTMENT OF HOMELAND SECURITY

Mr. VERDERY. Of course.

Chairman Camp, Chairman Gibbons and other members of the committee, thank you for the chance to be here today to join with General Hughes to testify about the efforts of the Department of Homeland Security to analyze and disrupt the travel of potential terrorists.

The 9/11 Commission noted that, and I quote, "targeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence operations and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators and constrain terrorist mobility". The administration and this Department concur with this observation, and we have implemented a number of successful programs to deny terrorists the ability to travel freely into the U.S., identify potential travel facilitators, and constrain their mobility.

This is a complex multiagency undertaking, and we are working in close collaboration with our interagency partners on this important task. We are reviewing how travel documents are produced and reviewed so we can better detect altered and fraudulent ones; improving and expanding watch-lists; and exploring ways to share data with our foreign counterparts that can help identify and thwart terrorists, and, of course, these efforts are designed to protect and respect the civil liberties and privacy of U.S. Citizens and residents, and of our visitors.

I believe General Hughes in his written testimony ably described the role of Information Analysis Section of DHS in participating in the Intelligence Community. It is absolutely critical that actionable intelligence and actual information be provided to the front-line components of DHS, whether it is an inspector at a port of entry, a Federal air marshal, an aviation screener or a criminal investigator, and that capability is robust and improving.

The BTS Directorate is current operations unit is responsible for ensuring a continuing productive relationship between the intelligence arms of BTS—Customs and Border Protection, Immigration and Customs Enforcement, and TSA—and IAIP. BTS analysts are assigned to IA, and there is a daily exchange of information between BTS agencies, IA and, of course, the Coast Guard. BTS analysts conduct follow-up research involving BTS incidents of interest and the Intelligence Community, and we have essentially set up a two-way street of information sharing where our components receive information immediately through IA, and IA is immediately alerted to significant operational activity.

Let me focus briefly on some of the programs we think are really disrupting the patterns of terrorist travel. And I will focus on the National Targeting Center, US-VISIT and our efforts to find fraudulent travel documents.

The National Targeting Center, operated by DHS's U.S. Customs and Border Protection, working with numerous Federal agencies, provides tactical targeting and analytical research support for passenger and cargo targeting in the air, sea and land operations in inbound and outbound environments.

NTC develops tactical targets, potentially high-risk people or shipments that should be subjected to additional scrutiny by CBP personnel, from raw intelligence, trade, travel and law enforcement data via the Automated Targeting System (ATS). The NTC supports DHS field elements including our container security personnel in 25 countries around the world, our visa security officers in Saudi Arabia, the CBP officers at ports of entry, and the Border Patrol, and is also working to support the pilot Immigration Security Initiative (ISI) operating in two airports in Europe to work on vetting passengers before they leave for international flights.

During the heightened threat period last December and throughout the winter, NTC played a pivotal role in analyzing advance passenger manifest information related to several international flights of interest that were deemed to be at risk in order to secure those flights. DHS is committed to improving the current collection of manifest information over the coming months by standardizing formats, requiring departure information for outbound flights and finalizing crew manifest requirements, and these requirements will

build on the passenger name record, or so-called PNR, data used for screening passengers. I personally served as the lead negotiator for the U.S. in our successful negotiations with the European Union that now allow that data to be transferred from Europe to DHS for analyzing incoming passengers.

The US-VISIT program is a continuum of identity verification measures beginning overseas with the visa issuance process operating at 206 nonimmigrant posts, 115 airports and seaports of entry. Secretary Ridge deserves great credit for moving ahead with biometric components of this system ahead of schedule.

And just to briefly summarize, as of the first 9 months of operation, we have now detected 838 individuals identified by the biometrics alone at ports of entry as subject to a watch-list information or other lookout, and about a third of those have had adverse action taken against them, being refused entry or being arrested. In addition, today, September 30th, is the first day the travelers in the Visa Waiver Program are being enrolled in US-VISIT.

The Commission's report noted that terrorists use altered and counterfeit travel documents to evade detection. Just yesterday I toured the ICE forensic document lab in northern Virginia. We have accumulated 130,000 legitimate and forged travel identification documents. They are accessible in seconds. The analysts at FDL develop hundreds of document alerts. They are sent to border inspectors, have the capability for front-line inspectors to have real-time review of suspect documents, and provides forensic investigation support and training. And I would encourage all Members interested in this issue to travel to northern Virginia to take a look at the FDL. It is truly a unique resource.

Hopefully during the question-and-answer period we can talk a little bit about lost and stolen passport issues. We are addressing those through Interpol, through technology development and through our review of the Visa Waiver countries. This is a critical, critical program to secure those documents.

Terrorism attacks in Asia, Europe and elsewhere are vivid reminders to us that terrorism is an international threat that cannot be conquered alone. We understand we must engage in a global effort each day through collaboration, information sharing and ongoing dialogue to bring the weight of our collective law enforcement intelligence capabilities to bear against those who seek to do us harm.

Thank you for the opportunity to be here. I will look forward to your questions.

Mr. CAMP. Thank you very much.

[The statement of Mr. Verdery follows:]

PREPARED STATEMENT OF C. STEWART VERDERY, JR.

Chairman Camp, Chairman Gibbons, Ranking Members Sanchez and McCarthy, and other distinguished members, I am pleased to be here today to testify about the efforts of the Department of Homeland Security (DHS) to analyze and disrupt the travel of potential terrorists. I am especially pleased to be joined by my colleague, Assistant Secretary Patrick Hughes, from DHS's Information Analysis and Infrastructure Protection Directorate (IAIP).

The 9/11 Commission noted that "[t]argeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility."

The Administration and DHS concur with this observation and have implemented a number of successful programs to deny terrorists the ability to travel freely into the U.S., identify potential travel facilitators, and constrain the mobility of known and suspected terrorists.

This is a complex multi-agency undertaking, and DHS works in close cooperation with its interagency partners on this important task. DHS works cooperatively with our colleagues at the Departments of State and Justice and the intelligence community to improve our ability to identify terrorists without impeding legitimate trade and travel.

We are reviewing how travel documents are produced and reviewed so that we can better detect altered and counterfeit documents, improving and expanding watch lists and how they are vetted, and exploring ways to share data with our counterparts that can help identify and thwart terrorists. These efforts are also designed to protect and respect the civil liberties and individual privacy of U.S. citizens, residents, and visitors.

I would like to focus today on our creation and use of the National Targeting Center (NTC) to identify both potential terrorists and patterns of terrorist travel, our US-VISIT biometric screening system which helps to fix the identities of individuals entering and departing the U.S., and our efforts to detect fraudulent travel documents. As described more fully in Assistant Secretary Hughes's testimony, I will also briefly address how we analyze and pass intelligence information to and from our border officers.

National Targeting Center

The NTC began around-the-clock operations on November 10, 2001, providing tactical targeting and analytical research support for anti-terrorism efforts. The NTC is primarily staffed by DHS's Customs and Border Protection (CBP). The NTC staff consists of CBP Officers and field analysis specialists who are experts in passenger and cargo targeting for air, sea, and land operations in the inbound and outbound environments. The NTC develops tactical targets—potentially high-risk people and shipments that should be subject to additional scrutiny by CBP personnel—and it develops these targets from raw intelligence, trade, travel, and law enforcement data.

The NTC has access to over 20 critical anti-terrorism and law enforcement databases, including the Terrorist Screening Data Base (TSDB) maintained by the Terrorist Screening Center (TSC), and receives strategic intelligence daily from CBP's Office of Intelligence, our IAIP Directorate, and other law enforcement and intelligence entities. The NTC includes representatives from ICE, the FBI, the intelligence community, the Transportation Security Administration (TSA), US-VISIT, the Department of Energy, the Department of Agriculture, the Food and Drug Administration, and the United States Coast Guard.

NTC supports DHS field elements, here and overseas, including Container Security Initiative (CSI) personnel stationed in 25 countries throughout the world, the Visa Security Program, and CBP Officers at all of our ports of entry, as well as between the ports through support to CBP's Office of Border Patrol. NTC also supports the Immigration Security Initiative, currently operating at Schiphol Airport in Amsterdam and Warsaw, Poland, where teams of CBP officers are deployed to work with local authorities in preventing the onward movement of people identified as presenting a security threat to the carrier or passengers on international flights destined to the U.S.

During the period of heightened alert last December, the NTC played a pivotal role in analyzing advanced passenger information system (APIS) manifests related to several international flights that were determined to be at risk, in order to ensure that passengers on board did not pose risks to the flights.

The NTC uses the Automated Targeting System (ATS) to identify and target high-risk passengers and cargo entering the United States. ATS permits the NTC's trained personnel to process advance passenger information, to recognize anomalies and "red flags" and to determine which individuals and shipments should be given greater scrutiny at our ports of entry.

DHS is committed to improving the current collection of passenger manifest information over the coming months by standardizing entry information formats, requiring departure information, and finalizing crew manifest requirements.

The United States and the European Commission signed an international agreement on May 28, 2004 permitting CBP to access passenger name record (PNR) data to be used for screening passengers. I personally served as the lead for the U.S. interagency team which negotiated for over one year until we succeeded in establishing a mutually acceptable legal framework to allow CBP to receive PNR data from the airlines that carry passengers between Europe and the United States. In

1996, the European Parliament and Council issued a "Data Protection Directive" that set forth detailed requirements for the utilization and sharing of personal data. Prior to our resolution of these issues with the Commission, airlines found themselves in a position where they could be subject to fines from EU member states if they provided PNR data to the United States.

PNR information is just one of many tools used by CBP to fulfill its mission. PNR data is an essential tool allowing CBP to accomplish its key goals: (1) PNR data helps us make a determination of whether a passenger may pose a significant risk to the safety and security of the United States and to fellow passengers on a plane; (2) PNR data submitted prior to a flight's arrival enables CBP to facilitate and expedite the entry of the vast majority of visitors to the United States by providing CBP with an advance and electronic means to collect information that CBP would otherwise be forced to collect upon arrival; and (3) PNR data is essential to terrorism and criminal investigations by allowing us to link information about known terrorists and serious criminals to co-conspirators and others involved in their plots, as well as to potential victims. Sometimes these links may be developed before a person's travel, but at other times these leads only become available days or weeks or months later. In short, PNR data helps CBP fulfill its anti-terrorism and law enforcement missions and allows for more efficient and timely facilitation of travel for the vast majority of legitimate travelers to and through the United States. At this time, CBP is receiving PNR data, which is enabling us to link information about known terrorists.

Over the course of our negotiations, both sides worked together to reach a workable solution that outlines the type of data that may be transferred, the period of time it can be retained, and the purposes for which it may be used. Additionally, the final arrangement includes requirements for aggressive and important passenger redress mechanisms, including a channel for direct access by European Data Protection Authorities to the Chief Privacy Officer at the Department of Homeland Security on behalf of European citizens.

While this agreement was signed by the EU and the Secretary of Homeland Security in May, matters related to the agreement are currently being challenged by the European Parliament before the European Court of Justice. We are, nevertheless, confident that the agreement is legally sufficient and will improve the safety of air passengers.

In addition, CBP continues to work on a version of ATS that, for the first time, will be able to identify potentially high-risk passenger vehicles and travelers at our land border ports of entry. The new version of ATS will also increase the amount of government data that the system can access and analyze and enable us to train more people on the use of the system.

These, and many other U.S. intelligence analysis capabilities, are being used to help exploit terrorists' vulnerabilities as they travel and to learn more about their activities and methods. In addition to our ongoing efforts to target terrorist travel to, from, and within the United States, the Administration is seeking, on both a bilateral and multilateral basis, to promote similar efforts by other responsible governments, and to provide those governments with relevant terrorist-related information.

US-VISIT

Prior to the terrorist attack on September 11, Congress twice mandated the creation of an electronic entry-exit system. Following the events of September 11, Congress added the requirement that the entry-exit system focus on biometric technology as a means to verify the identity of foreign travelers. DHS established the US-VISIT program, and began implementing US-VISIT, as required, at 115 airports and 14 seaports of entry on January 5, 2004. In accordance with direction from the Secretary, US-VISIT incorporated biometric technology into US-VISIT even though biometrics were not statutorily mandated by that date.

US-VISIT enhances the security of our citizens and visitors; facilitates legitimate travel and trade; ensures the integrity of our immigration system; and protects the privacy of our visitors.

In addition to developing an integrated system that records the arrivals and departures of travelers and uses biometric technology to combat fraud, DHS is designing US-VISIT to: (1) provide information to CBP Officers and consular officers for decision making purposes; (2) reflect any pending or completed immigration applications or actions; (3) identify nonimmigrant overstays; and (4) provide accurate and timely data to appropriate enforcement authorities. US-VISIT is working to accomplish these objectives.

US-VISIT represents a major milestone in enhancing our nation's security and our efforts to reform our borders. It is a significant step towards bringing integrity

back to our immigration and border enforcement systems. It is also leading the way for incorporating biometrics into international travel security systems.

US-VISIT is a continuum of security measures that begins before individuals enter the United States and continues through their arrival and departure from the country. Enrolling travelers in US-VISIT using biometric identifiers allows DHS to:

- *Conduct appropriate security checks:* We conduct checks of visitors against appropriate lookout databases, including the TSDB, and selected criminal data available to consular officers and CBP Officers at the ports of entry, including biometric-based checks, to identify criminals, security threats, and immigration violators.
- *Freeze identity of traveler:* We biometrically enroll visitors in US-VISIT—freezing the identity of the traveler and tying that identity to the travel document presented.
- *Match traveler identity and document:* We biometrically match that identity and document, enabling the CBP Officer at the port of entry to determine whether the traveler complied with the terms of her/his previous admission and is using the same identity.
- *Determine overstays:* We will use collected information to determine whether individuals have overstayed the terms of their admission. This information will be used to determine whether an individual should be apprehended or whether the individual should be allowed to enter the U.S. upon her/his next visit.

The DHS and Department of State (DOS) together have created a continuum of identity verification measures that begins overseas, when a traveler applies for a visa, and continues upon entry and exit from this country. The system stores biometric and biographic data in a secure, centralized database and uses travel and identity documents to access that information for identity verification and database checks. 206 nonimmigrant visa-issuing posts and 118 immigrant visa issuing posts capture finger scans and digital photographs of foreign nationals when they apply for visas, regardless of their country of origin. This process will be implemented at all 207 visa-issuing posts worldwide by October 26. In addition, today is the first day that nationals from Visa Waiver Program (VWP) countries will be enrolled in US-VISIT when they travel to the United States.

At assigned U.S. border points of entry, designated visitors are required to provide biometric data, biographic data, and/or other documentation. This data is checked against various databases, which US-VISIT has successfully integrated and which contain visa issuance information, terrorist (through the TSDB) and criminal watchlists, and immigration status information. That information allows a CBP Officer at the border to verify the identity of the traveler and to determine whether the foreign national is a public threat or is otherwise inadmissible. In its first 9 months of operation, DHS processed over 8.9 million foreign national applicants for admission through US-VISIT at its air and sea ports of entry. During that period, 838 individuals were identified by biometrics alone as being the subject of a watchlist lookout. After a careful examination of all the relevant facts, DHS elected to take adverse action in approximately 33 percent of those cases where an individual was identified—such action included arrest or refusal of entry into the United States.

Examples of US-VISIT Success

For example, At Newark international airport, an international traveler appeared for inspection. Standard biographic record checks using a name and date of birth cleared the system without incident. However, a scan of the traveler's index fingers, checked against the US-VISIT biometric database, revealed that the traveler was using an alias and was, in fact, a convicted rapist. Additionally, he had previously been deported from the United States. US-VISIT's search disclosed that the individual used at least nine different aliases and four dates of birth. He had previously been convicted of criminal possession of a weapon, assault, making terrorist threats, and rape.

CBP Officers at JFK International Airport processing a passenger through the US-VISIT procedures found that the individual was using an alias. Further information uncovered two arrests for aggravated trafficking of drugs, a subsequent failure to appear, and visa fraud. The traveler had used this fraudulent visa to enter the United States over 60 times without being detected by standard biographic record checks, the last time only 11 days earlier.

Recently, a traveler with four aliases, three social security numbers, and a criminal history going back to 1990, tried to enter the United States. He was not admitted because a comparison of his fingerscans against the US-VISIT biometric watch list determined that he had previously been deported from the United States.

US-VISIT, as well as the student tracking system SEVIS, has developed mechanisms to facilitate the lawful and appropriate use of entry-exit data by law enforcement agencies such as the Federal Bureau of Investigation to enhance their ability to investigate terrorist travel patterns.

Secure Flight

On August 26, DHS unveiled the concepts underlying our new Secure Flight program designed to improve security for domestic flights by improving the use of terrorist screening information. Under Secure Flight, TSA will take over responsibility for comparing PNR information of domestic air passengers to a greatly expanded list of individuals known or suspected to be engaged in terrorist activity—a function currently administered by each airline individually. The move will help reduce the number of false alerts caused by the current outdated system.

When in place, following the completion of a pilot program and consideration of any issues that arise, and after the completion of a rulemaking, Secure Flight will help move passengers through airport screening more quickly and decrease the number of individuals selected for secondary screening—while fully protecting passengers' privacy and civil liberties.

This new system will implement a key recommendation of the 9/11 Commission for the government to continue improving the use of 'no-fly' and 'automatic selectee' lists by using the terrorist screening database maintained by the Terrorist Screening Center.

Significant progress has already been made by the U.S. Government by providing greatly expanded No-Fly and Selectee lists to airlines to conduct checks on their own computer systems under the current prescreening program. New names are being added every day as intelligence and law enforcement agencies submit persons for consideration. As Secure Flight is phased in, TSA will be able to check passenger records against sensitive watch list information not previously available to airlines.

Secure Flight differs from earlier enhanced prescreening systems by focusing screening efforts on identifying individuals known or suspected to be engaged in terrorist activity, rather than using it for other law enforcement purposes. As with previous proposals, the new program will also include a redress mechanism through which people can resolve questions if they believe they have been unfairly or incorrectly selected for additional screening.

The development of the program will be as publicly transparent as possible without compromising national security. Testing and eventual implementation will be governed by strict privacy protections including passenger redress procedures, data security mechanisms, and limitations on use.

Privacy-related documents and a proposed order compelling the submission of historical PNR data from the airlines to TSA for testing the Secure Flight program were released for public comment and published in the Federal Register on September 24. The notice addressed the purpose of the testing and set forth the limited purposes for which the information collected will be used in Secure Flight.

Alien Flight Students

On October 5, 2004, TSA will assume the responsibility from the Department of Justice for the Alien Flight Student Program (AFSP) program and conduct security threat assessments on all non-U.S. citizens who apply to receive flight training from an U.S. flight school.

Flight schools are required to submit training information, such as the type of training the candidate is requesting, and biographical information, including full name, passport and visa information. Applicants must also provide their fingerprints.

All non-U.S. citizens who apply to U.S. flight schools will now have to undergo a security threat assessment regardless of the size of aircraft in which they wish to train. Previously, only students wishing to fly aircraft of 12,500 pounds or more underwent threat assessments. Another significant change is that flight schools will be required to submit a candidate's photograph to TSA when the candidate arrives at the flight school to help ensure the person who was cleared by TSA is the person who actually receives the flight training.

Human Smuggling and Trafficking Center

In July, DHS and the Departments of State and Justice established the Human Smuggling and Trafficking Center. The center is housed at the State Department and includes the participation of intelligence agencies.

The Center analyzes and disseminates information, and provides related support to law enforcement, intelligence, diplomatic, foreign assistance, and other entities that take action against the threats of human smuggling and trafficking and against criminal support for terrorist travel.

The Center is another measure that the Administration has taken to improve our ability to analyze and disrupt terrorist travel, and we are optimistic about its possibilities.

Deterring the Use of Fraudulent Documents

The Commission's report noted that terrorists use altered and counterfeit travel documents to evade detection. In the border and immigration enforcement arenas, biometric identifiers are tools that help prevent the use of fraudulent identities and travel documents. The purpose of the biometric identifier is to verify a person's identity in order to run criminal history checks and to ensure that an individual cannot apply and/or be granted benefits under different names. Biometric visas issued by the DOS to travelers to the United States allow one-to-one matches, to verify that the person presenting the visa is the person who was issued the visa, and one-to-many matches, to ensure that the bearer is not the subject of a biometric lookout or enrolled in the system under another name. Like the biometric visa process, US-VISIT enrollment fixes a person's identity. When a VWP traveler enrolls in US-VISIT, the person's fingerprints will be electronically linked to the passport, thus preventing another person from using that passport by freezing identities at the border and ensuring that the person is not enrolled under another name.

CBP Officers must use their expertise to recognize and block the fraudulent use of many types of identification documents presented by applicants for admission at our ports of entry. For example, there are more than 240 different types of valid driver's licenses issued within the United States, and more than 50,000 different versions of birth certificates issued by U.S. States, counties, and municipalities.

While advances in technology allow our dedicated and hardworking CBP Officers to examine and validate documents presented for reentry, that same technology also enables the perpetrators of fraud to produce, relatively inexpensively, high-quality fraudulent documents. Forgers and counterfeiters can produce high-quality fake birth certificates and driver's licenses with off-the-shelf software programs and materials that are difficult to detect without sensitive instruments and sufficient time to examine them.

Our CBP Officers are also charged with detecting look-a-likes or impostors who attempt to use valid documents which belong to another person. This is one of the fastest growing phenomena in travel document abuse. Document vendors solicit genuine, unaltered documents and match them up with "look-a-likes." DHS's Immigration and Customs Enforcement (ICE) has developed a training program to detect impostor documents, which it has conducted for both U.S. and foreign immigration and border officers around the world.

Equipment costs money, and taking the time to examine thoroughly and in-depth every one of the approximately 460 million identity documents presented at our over 300 land, sea, and air ports of entry would be an enormous undertaking with potentially serious secondary effects. And, even were we to do this, this effort would only permit us to detect fraudulent documents, not, legitimately issued documents that are based on fraudulent identity.

The Administration continues to improve efforts in the area of identification security. Last month, the President signed Homeland Security Presidential Directive-12 (HSPD–12) to set a common identification standard for Federal employees and contractors. HSPD–12 mandates the expedited, public, and open development of a uniform standard for Federal employee and contractor identification that ensures security, reliability, and interoperability; closes security gaps and improves our ability to stop terrorists and others from accessing or attacking critical Federal facilities and information systems; and improves efficiency among Federal agencies through more consistent systems and practices.

Secure identification is a priority for the United States. As noted by the 9/11 Commission, birth certificates, drivers' licenses, and most other forms of identification have traditionally been issued by State and local governments, not the Federal Government.

At the Federal level, we are working closely with our State and local partners to find ways to strengthen the standards used to issue documents that people use to establish their identity without creating a national identity card. DHS has supported the efforts of the American Association of Motor Vehicle Administrators (AAMVA) in looking at the security of drivers' licenses and strongly supports the States in their endeavors to improve the security of these documents.

Lost and Stolen Passport Data

DHS is addressing security challenges posed by lost and stolen passports together with our colleagues in the Department of State, who are responsible for the U.S. passport system, and our foreign counterparts.

CBP complies with the section of the Enhanced Border Security and Visa Entry Reform Act of 2002 which requires that lost and stolen passport data be entered into lookout systems within 72 hours. CBP incorporates lost and stolen passport information into its systems to aid in the detection and interception of persons using lost and stolen documents.

Across the globe, international border control authorities continue to seek timely and accurate information concerning the validity of travel documents presented at consular posts and their borders. In most cases, countries are able to recognize the misuse of their own documents, but because of concerns about the use of personal data, many nations remain reluctant to share data on lost or stolen travel documents with other governments or international agencies.

We are making progress in our efforts to encourage international cooperation in this area. For example through the efforts of the Departments of State and Justice, the U.S. has provided over 300,000 records of lost and stolen passports to the Interpol's lost and stolen document database, which is available to border authorities worldwide. We hope that many more of our international partners will join us in this effort.

We are working with our colleagues at the Department of State to exchange of information with the Government of Australia on lost and stolen passports. We expect that an agreement—the first of its kind will be concluded shortly. Efforts are also under way internationally to enhance such exchanges of information. At the June 2004 G8 Summit in Sea Island, G8 partners agreed to a U.S. proposal to start providing information on lost and stolen passports to the Interpol database by December 2004. This will allow participants access to real-time information on lost and stolen international travel documents. We want to advance this effort beyond the G8 and encourage all countries to submit relevant information to the Interpol database. We are promoting a comparable initiative among the APEC countries to develop Regional Movement Alert System.

Additionally, the U.S. is initiating a study to assess a technology concept that could further address this concern. The Enhanced International Travel Security (EITS) concept would use distributed databases as a mechanism to allow real-time exchange of the basic information needed—i.e., a "yes" or "no" response—to assess the validity of a document without requiring visibility into the actual data used for that determination. The approach would be similar to the one already used worldwide by the banking industry to support ATMs. Developing better systems for international sharing of information, and expanding participation to more countries will improve our ability to identify and screen travelers before they enter our country.

In addition, as DHS conducts the required reviews of countries participating in the Visa Waiver Program, each country has provided detailed information about lost and stolen passports, their law enforcement response to such incidents, and efforts made to tighten distribution and document security processes. How a country handles this key issue will be an important factor in how DHS, working with interagency teams, determines whether VWP countries shall remain eligible for the program. These reviews are due to be completed in October.

Integrating Intelligence Information

DHS has developed sophisticated methods for identifying and targeting potentially high-risk cargo and passengers through the effective use of strategic intelligence. This intelligence is gained through a close relationship between our bureaus, ICE, CBP, and the Transportation Security Administration (TSA), our IAIP Directorate, the U.S. Coast Guard's intelligence program, and the intelligence community. As a result of these relationships, we are able to review, analyze, and integrate information that resides in multiple government databases, various watch lists, and advance information received directly from travelers, airlines, and shippers.

BTS's Director of Current Operations is responsible for ensuring a continuing productive relationship between the intelligence arms of our BTS agencies—CBP, ICE, and TSA and IAIP. BTS analysts are assigned to IA and there is a daily exchange of information between the BTS agencies and IA. BTS and the Coast Guard have also exchanged personnel to enhance data sharing.

The BTS analysts primarily conduct follow-up research concerning BTS incidents of interest to IA and the intelligence community. This relationship provides a two-way street of information sharing, where the component representatives are immediately alerted to significant information received through IA channels and IA is immediately alerted to significant operational activity.

BTS intelligence representatives attend multiple, daily, meetings with IA where significant intelligence information is discussed. This includes intelligence derived from other elements of the intelligence community and law enforcement entities.

BTS agencies send daily reports to IA about significant incidents encountered by BTS agencies. These incidents are usually associated with a watch listed individual intercepted at the border, a subject on the no-fly list attempting to board an aircraft, or information alleging potential terrorist-related activity gained from an investigation.

BTS also works with IA to vet intelligence bulletins, reports, and assessments and to jointly assess relevant information. BTS ensures that intelligence is shared between intelligence analysts and operational personnel. BTS seeks to "operationalize" the intelligence we receive to ensure that the intelligence is incorporated into targeting and other decisions on an ongoing basis. For example, we may institute more targeted secondary inspections of travelers from regions that intelligence suggests warrant additional scrutiny, send priority leads based on intelligence to investigators in the field, or reassign Federal Air Marshals.

ICE has created a Threat Analysis Section (TAS) to identify and address potential vulnerabilities relative to the national security of the United States. The TAS establishes associations between individuals or groups linked to potential national security threats, develops profiles based upon relevant investigative and intelligence reporting, and produces actionable leads for field offices.

In addition, TSA's Transportation Security Intelligence Service (TSIS) produces a daily intelligence summary and a weekly suspicious incidents report that is shared with Federal Security Directors Federal Air Marshals, and state, local, and industry transportation stakeholders.

Conclusion

We have made much progress to deny terrorists the ability to travel freely into the U.S., identify potential travel facilitators, and constrain the mobility of known and suspected terrorists. In addition to the initiatives described above, we are working aggressively with our international partners to improve standards for travel documents, enhance aviation safety and port security, and speed the exchange of terrorist identifying information. The bombings in Madrid, the recent hostage crisis in Beslan, Russia and the Australian Embassy bombing in Jakarta also serve as vivid reminders to us that terrorism is an international threat that cannot be conquered alone. DHS understands that we must engage in a global effort each day, through collaboration, information sharing and ongoing dialogue to bring the weight of our collective law enforcement and intelligence capabilities to bear against those who seek to do us harm.

I would be happy to answer any questions you have at this time.

Mr. CAMP. Thank you both for your testimony.

General Hughes, given your extensive experience in intelligence and your understanding of this threat to our homeland, which, since 9/11, we have been focused on very intensely, how do you characterize our efforts to track potential terrorists attempting to enter the United States? How would you particularly—you know, in comparison to pre-9/11?

Mr. HUGHES. Well, I think it is much improved; for one thing, the fact that we have standing watch-lists as a tool which we did not have before. The fact that we have a variety of registration techniques and much better overwatch on travel documentation, the issuance of passports and visas and certain knowledge provided by the travelers in many cases about who they are and what they intend to do in their travel is a big change. That does allow us to begin to have knowledge of them earlier in the process than we used to. I think the Department of State may have had that information, but it wasn't integrated into the intelligence and law enforcement and security communities in a way that it is now.

When they reach our borders, of course, as Stewart was discussing here, the U.S. visa—excuse me—the US-VISIT program, the enhanced Customs and Border Protection mechanisms at the border when they seek passage into our country, and the knowledge that we have about them combined is a very powerful tool, and indeed we are—as opposed to tracking them, in many cases we are interdicting them earlier. We are interdicting them in some

cases before they get on an airplane. Occasionally that system fails. When they reach our border, generally we know who they are, and we are finding them.

I will say that we have some additional capability from the past in the illegal border-crossing context. We know quite a lot about activities to our Southwest border and Mexico, and some information concerning along the Canadian border, perhaps a little bit less in the case of Canada because of the construct between our two countries. But that is a very powerful tool. We can in many cases anticipate movement, and we often do interdict persons on those two borders because we knew something about them. We knew they were staging or a group was planning to travel or something like that. It is not perfect, and I don't wish to communicate to you it is by any means, but it is better than it used to be.

And the last thing I would like to mention to you is the term ″tracking″ is very interesting. We have not only this foreknowledge or preknowledge of their activities in many cases, but we are then able to amass this knowledge in a cumulative way in databases that did not exist before. This is an invaluable tool and critical to our future success in this regard. The identification and registration in these databases of these people is vital, and we weren't doing that in the robust way that we are now doing it.

Mr. CAMP. I appreciate that, and I think we all agree that we have been working toward putting together a really strong system in place to apprehend terrorists trying to enter the United States. But it seems to me the more we strengthen our policy at ports of entry, it is also more likely that terrorists may try to infiltrate the country simply by walking across our border. You know, Time Magazine recently had a fairly chilling article on this issue and the human smuggling operations and the efforts like that.

What is the Department doing—and this may be something the Assistant Secretary would like to comment on as well. What is the Department doing to strengthen our capabilities to prevent illegal crossings, and how can we use intelligence information to target and detect potential terrorists who may be trying to enter our country in that fashion?

Mr. VERDERY. Well, the short answer is a lot. And at some point I would like to follow on to what General Hughes talked about in terms of our overseas efforts, and especially on the visa side and US-VISIT.

In terms of the southern border, the enforcement capabilities are growing by leaps and bounds, but it is obviously a very difficult problem. In recent years, we have increased the number of Border Patrol agents. We have increased the use of advanced technology, UAVs, sensors, lighting, motion detection and the like. We have put the necessary number of prosecutors and asylum adjudicators and the like on the ground, as well as advanced aircraft deployment. All this, though, does demonstrate this is a difficult issue with the amount of traffic across the border.

Under Secretary Hutchinson has launched the Arizona Border Control Initiative, ABC, which is really trying to bring operational control to certain sectors in Arizona and has resulted in huge increases in the number of apprehensions in that sector. But that, of course, has then put pressure on other sectors who have had to re-

spond with efforts such as the Los Angeles Airport Initiative to try to keep migrants from being moved into LAX and then flown into other parts of the country.

We also have to look at our legal authorities, and that is why we put into place the expedited removal program to turn around third-country nationals quickly who don't have asylum claims; and the interior repatriation program, to fly Mexicans back into the interior of the country to try to break the cycle of people being just returned across the border. But over the long haul, we, of course, need to improve the entire spectrum of apprehension capability, detention capability, removal capability. It is a long-term project that we all have to concentrate on.

General HUGHES. May I just comment on the intelligence piece of this answer? In this open environment, it is important for me to tell you that especially with Canada and Mexico, but also with some other countries that are involved, not in crossing the border illegally as in walking across, but the illegal border crossing activity can be facilitated from afar through the use of illegal documentation and false identity. And we do have better and growing cooperation with both Canada and Mexico and with other countries in that regard. Once again, in an open environment I probably wouldn't like to get into the details, but I can look you directly in the eye and tell you that it is better than it was. It needs to get better than it is, and we are working on that part of this activity.

Mr. CAMP. All right. Thank you. Thank you both very much.

And at this time the Chair would recognize the Ranking Member of the Border and Infrastructure Subcommittee Ms. Sanchez to inquire.

Ms. SANCHEZ. Thank you, Mr. Chairman. And thank you gentlemen for being before us.

I think the last few weeks in particular, the Department of Homeland Security has had some pretty negative press with respect to borders and air; borders, I think, because Time Magazine, I believe, was one that has that little picture of something being pulled apart and talked about, how much we really do need to do with respect to our borders. And it really did highlight the northern border, which, of course, we all know is much more open than even the southern border. But I think the other incident that happened was the incident of Yusuf Islam, who everybody in this room probably knows as Cat Stevens. He had—you guys returned him to England after he arrived in the United States because his name was on the watch-list.

I think this episode highlights several problems with our current policy, and I sort of want to go through them so I understand what happened. I think America wants to know what happened and what we are going to do to fix this.

First of all, he was allowed to board the plane, and I guess while he was en route, you guys found his name on a watch-list. I guess the question is why would you—why wouldn't we be checking it before we got a supposed dangerous person on the plane, because maybe he could have blown it up as we were trying to figure out who he was? So the question is why do we have such a huge security gap in the Visa Waiver Program that allows travelers participating in the Visa Waiver Program to get on a plane without first

being run through the watch-list check? And why doesn't DHS check the names of passengers on international flight against the terrorist watch-lists before the flights take off? And if you can't do it to all passengers, can you at least do it for the vast majority of passengers who buy international tickets at least an hour in advance?

Mr. VERDERY. I think I will take that one, Congresswoman. The Cat Stevens episode does exemplify a current weakness in the way international travelers come to this country. As you know, we do not have people stationed overseas except for a couple of selected airports, as I mentioned, and or the Immigration Security Initiative. And essentially the airlines are currently our response overseas to enforce the watch-lists. And so when a person such as this individual is on a watch-list, it is the airlines' responsibility to compare the manifest against the watch-list and make those no board determinations.

In this case there was an error made. We recognize this weakness and have announced as part of the Secure Flight Initiative For Domestic Travel that the international realm will be enhanced by a proposed rule to be announced later this year to require that manifest information be supplied to us in advance of wheels up, so before the plane takes off. Now, this would be a very complicated endeavor. It will not only change the way booking patterns are made, especially connecting flights from overseas travel, but it would provide much greater security for us to be able to run those watches ourselves through the National Targeting Center before the plane takes off, and hopefully these types of situations will be much less likely to occur.

You asked about the Visa Waiver Program. Again, the watch-list check that is done now is no different whether you are from a visa waiver or non-visa waiver country. This same error could occur with the airlines enforcing the system. So that is not the issue in this case. There is a visa waiver issue we can discuss at another time.

We do have the ability, and this happened during the heightened threat period in the winter, if there is a plane under a certain threat, we can essentially hold the plane on the tarmac and run the checks, and that is what was going on. But that is not a tenable solution for all international travel, and that is why we were going to move with this proposed rule to try to get this information ahead of time. It is also why we went to such great lengths to get the PNR, kind of back-up information about your travel agent, the people you are flying with, your bags, and your frequent flyer number from the Europeans under this agreement, so we could use that investigative tool both to find people and also to clear people if there is a potential hit.

Ms. SANCHEZ. You held him for 33 hours. You held his daughter for 33 hours also, because they ended up going off together. After 33 hours you sent him back to England. In 33 hours you couldn't figure out who this guy was? I mean, such a famous person? I am trying to figure out what kind of a system are we using to figure out what is going on here. And did you tell the British authorities? Why would you put him on a plane if he was such a dangerous per-

son? Did you put him on chained; you know, shackled? I mean, what is the process?

Mr. VERDERY. Well, there is a lot of different issues involved in the situation. I mean, there is the 'should he have been allowed on the plane' issue. There, is the 'what should the plane have done while it was in midair'; and then there is 'how was the individual who actually makes it to our country who is on a no-fly list or a watch-list treated'? They are all separate issues, and all need separate analysis.

But in this case, we feel that he was treated appropriately. He should not have been allowed on the plane, and we had to return him when he arrived in our country after the appropriate booking.

So we need to continue to work on these processes, but we feel that proper procedures were followed once we recognized that he had been allowed to board. And again, that demonstrates all the more why we need to make these decisions ahead of time before the person boards the plane.

Mr. CAMP. All right. Thank you very much.

Ms. SANCHEZ. Thank you Mr. Chairman.

Mr. CAMP. Thank you.

At this time the Chairman of the Intelligence and Counterterrorism Subcommittee Mr. Gibbons may inquire.

Mr. GIBBONS. Thank you very much, Mr. Chairman.

And, General Hughes, again, welcome. And I have read your testimony and wanted to ask a series of questions, if I may, because I think it will sort of hone itself down to or distill itself down to a point where I think we are going to get to the heart of the issue here, which is information analysis.

As you stated in your testimony, information analysis is really at the heart, I think, of good intelligence efforts, and absolutely, if you don't have good analysis, no matter how good the collection is, the result is going to be flawed. So my question is, is when you have several other Department—or components within the Department of human—or homeland defense that maintain distinct intelligence units, what kinds of control do you have as the head of the information analysis over these other intelligence offices? Is there a need for a structured relationship between IA and these offices? If there isn't one, should there be one? And tasking; describe for me the tasking ability of IA to these other offices in order that you get the right information to make a decision, from your standpoint.

General HUGHES. Well, the answer, sir, I think, is—I will start from the back and go forward here. The capabilities resident in all of organizations that I enumerate in my oral statement are impressive. They all produce what I would call organizational intelligence. They are focused on their organizations. The Secret Service, as an example, is exclusively focused on the missions and matters at hand for the Secret Service, and they are very closely held and are not broadly applied for very good reasons. Conversely, perhaps the United States Coast Guard, a member of the U.S. Intelligence Community in its own right, it is a bona fide member and has its own budgetary line and its own identity, has a very broad set of capabilities akin to any other armed force. And I will just describe one more example, Immigration and Customs Enforcement, which is—in large measure operates in a clandestine manner and is a

very capable organization in the human intelligence context, all of those and others that I won't take the time to enumerate, together, taken together, find their way into the national Intelligence Community through their own conduits and through the Department of Homeland Security. Depends on the circumstances, the nature of the reporting, but virtually everything of departmental and national interest comes to us at some point.

I believe we have a value added in regard to the analysis of all of that information. We are able to put it together, assemble it in one place, cause it to become synergistic in nature.

The answer to the last part of your question, sir, we can task anyone inside the Department of Homeland Security in the name of the Secretary, and we do.

Mr. GIBBONS. Is there a structured relationship between you and these other intelligence agencies?

General HUGHES. Yes, there is. We have an agreement among us which has been verified by the Secretary and by their individual organizational leaders that IA is the departmental organization that gives some form to the structure. We meet every 2 weeks formally in the Homeland Security Intelligence Group context, and we exchange information among us and between us. We also have coparticipation in many meetings, and interaction every day exists between us in automated form, like telephone and, in many cases, face-to-face meetings that occur because we interact.

Mr. VERDERY. Congressman, if I could just add on this from the BTS perspective. And that is one of the points of having the Border and Transportation Security Directorate as an umbrella over these large operational components, CBP, ICE, TSA, which have their own headquarters. They are operating around the country, around the world. BTS is at headquarters with IA, so there is constant interaction between General Hughes' operation and the BTS headquarters operation; and also to coordinate, because we recognize that the activities, intelligence or otherwise, between the BTS components are so linked, especially between ICE and CBP, because essentially Congress broke INS and Customs in half and stuck the investigators with the investigators and the inspectors with the inspectors. But those links between the two to bring front-line activity back to the investigative realm has to be maintained. And that is one of the large purposes of the BTS Directorate is to make sure that link continues, along with getting the intelligence from headquarters out to the field.

Mr. GIBBONS. Well, Secretary Verdery, let me ask you this: You just talked about having 838 apparent hits on your watch-list, with one-third receiving some sort of adverse action, either arrested or rejected for entry due to the biometrics program that you have got. What are you doing today to enhance the current capability of biometrics? In other words, are you looking at new technologies that are out there so that we don't get, as Ms. Sanchez said, an inadvertent hit because of the inability either to not have the information that was properly there, or to have a poor biometric system that doesn't do what we expect it to do? What programs, what pilot efforts have you got going? What research and development—are you reaching out to the private sector to do this?

Mr. VERDERY. Well, sir, the VISIT system which you referenced is obviously a fingerprint-, finger-scan-based system. Secretary Ridge, the Attorney General, and the Secretary of State made the decision to base it on fingerprints largely because that is how we have people listed in criminal databases, and also in terrorist watch-lists in many cases. That is what makes us able to find people, and it has worked extremely well. I think the turnaround time is running about 6 seconds from a systems perspective.

Mr. GIBBONS. There are also other systems out there that could be supplemental to the fingerprint systems that could be very helpful.

Mr. VERDERY. There are. VISIT is always looking at trying to find repetitive or back-up systems that would enhance the biometrics, such as the facial recognition. Part of the biometric passport which will be coming on line throughout next year will be part of the VISIT system. We have to deploy readers to read those biometric facial recognition parts of the passport and build that into the database. We are looking at other biometrics, whether it is iris or the like, and that can be built in on top of that.

Now, a very important thing, the President issued HSPD 11, Homeland Security President's Directive 11, last month, which requires our Department to go through a screening review of all things across the government, including biometric screening processes, to harmonize them to come up with the best biometrics, the best screening procedures to make them consistent. That review is ongoing right now with a biometric subgroup.

Again, the other thing I should mention, our Science and Technology Directorate, not represented here, is putting in an incredible amount of effort on next-generation biometrics, working with our operational entities like US-VISIT.

Mr. GIBBONS. Well, at some point I would like to talk to you personally about these systems and look forward to that.

Thank you, Mr. Chairman.

Mr. CAMP. Thank you.

And at this time the Chair recognizes the Ranking Member of the Intelligence and Counterterrorism Subcommittee Ms. McCarthy to inquire.

Ms. MCCARTHY. Thank you, Mr. Chairman.

I have a question for each one of you. I will take Mr. Verdery first. I appreciate that you said that we are not under the practice of holding planes when we are checking watch-lists. I happen to agree with you on that. But in a journey I made during the recess period, I learned that Australia has a system now where they do that investigation when the individual buys the ticket. And I wonder if we are moving in that direction on this legislation in the House, sponsored by our Ranking Member, to encourage that. Would you give us your thoughts?

Mr. VERDERY. Yes, ma'am. As I mentioned, we have announced that we are planning to promulgate a draft rule that would require that advance manifest information be supplied before the plane takes off so that we can do the vetting at the National Targeting Center before the plane gets into the air. And so that is something that will be coming down the pike.

And I will say, to be candid, it is not an easy solution, because if you talk to airports, airlines, the way that the changes have had to be made to how people book flights, the way people connect on flights will be immense. There will be costs here both in terms of inconvenience to passengers, the way airports are structured and the like. We support it, we think it is the right way to go, but it is something that has to be managed very carefully to make sure we don't kill off the travel industry in the process.

Ms. MCCARTHY. Well, it hasn't killed off the travel industry in Australia, so I think there is probably a good model for you out there. And people who are bargain shopping are generally buying their tickets ahead of time, and that should be of assistance in your efforts as well. I think it is only Members of Congress that don't know when they are getting on a plane.

Mr. VERDERY. It is of assistance, but, of course, when you are talking about millions of incoming travelers, even if you have a 1 percent error rate where you know you are talking to the travel agent on the phone and you say your name or an address or a phone number, and they mistype a key or a number, that then ends up with the kind of false hits that you try to avoid. So that is why the system right now is based on the information on your passport that is swiped electronically at the desk at the check-in counter so there aren't errors, or very rarely, in that kind of information taking. You take it off the phone, off the Internet, you end up with more errors.

Ms. MCCARTHY. Well, I have every faith that you will figure this out and will do an even better job than Australia.

General, does DHS or TTIC or any of the other intelligence agencies have an office devoted specifically to terrorist travel? The information sharing that is going on in other countries, I was on a trip with Member Dunn, who chaired the trip to Ireland, to Northern Ireland, the Republic of Ireland and England, and one of the examples we learned there was that a—of a police officer in Northern Ireland investigating an incident uncovered information that, when shared with others in the Republic of Ireland, in the South, and with Great Britain led to the discovery of the cell that funded the Bali tragedy and others. So they, albeit they are all in one compact series of islands, are doing that information sharing.

How are we doing on information sharing not just within our own country, but within those other strategic countries that are so important to our mutual success?

General HUGHES. That is a good question, but it is broader than the Department of Homeland Security. I will go ahead and answer it on behalf of the many other colleagues.

The U.S. Intelligence Community, at a variety of levels, especially the Central Intelligence Agency, the Department of State's intelligence organs, the Federal Bureau of Investigation, and the Defense Intelligence Agency, and the Department of Homeland Security, we all exchange information with other countries. It is not perfect in some cases. And the reasons are we have to go forward with information that can be released and placed at risk in the other countries' realm. We do have mechanisms to do that, such as tear lines and sanitization, where you take out the source's meth-

ods that we use to get the information. But it is a very robust activity and ongoing.

I think there was kind of an interior question there that you asked, and that is how are we doing with regard to the travel, terrorist travel focus? The Transportation Security Administrations intelligence organisms, there are two or three different pieces to that, do overwatch terrorist travel in a professional sense. And in my organization, as part of our Strategic Intelligence Division, we have a culmination of liaison officers and devoted analysts who work part time or whole time on the issue of terrorist travel. Indeed, I would probably say each and every day, my time is devoted in some measure to the issue of persons who we have encountered in the travel process who are connected in some way with terrorism. It is of vital importance to us.

Ms. MCCARTHY. Mr. Chairman, if I might pursue very, very briefly.

Mr. CAMP. Very briefly. The gentlewoman's time has expired.

Ms. MCCARTHY. Yes, sir.

Are you sharing this—is there a clear sharing with other countries?

General HUGHES. Yes.

Ms. MCCARTHY. Thank you.

Mr. CAMP. The gentleman from New Jersey, Mr. Andrews may inquire.

Mr. ANDREWS. Thank you, Mr. Chairman. I appreciate the testimony of the witnesses.

Our goal, our policy, is to reach a day when every person attempting to gain entry in the country can be affirmatively identified so we know who they say they are. When will we reach the day where every port of entry into the country has biometric reading capability?

Mr. VERDERY. Well, if you are talking about the US-VISIT biometric reading capability, that has been deployed to the major seaports. There are some smaller ones that have not been brought on line. That will be coming down the pike throughout the coming months and years. In addition to that gap, we are deploying at the land borders, at the 50 largest land borders, at the end of this year and the smaller ports of entry throughout next year. So US-VISIT is not a complete system by any means, but the Secretary, I think, took the bold step of deploying it in stages, because no one had been able to do this because no one—

Mr. ANDREWS. I understand. You want to do it right rather than fast. But we want to do it right and fast. So what percentage of people coming into the country today do not have their IDs biometrically read?

Mr. VERDERY. Well, I am trying to remember. The overwhelming number people who come in this country are coming via the land border, and the larger percent of that from Mexico. Now, most people coming from Mexico are Border Crossing Card holders. I would have to get the numbers for you, but my sense of it is at least probably a third of the individuals coming in are coming in as Border Crossing Cardholders, coming back and forth all the time. Those people have gone through a background check similar to a visa, so

they have been checked. Anybody who has gone through a visa has been checked. And now starting today—

Mr. ANDREWS. When you say checked, you mean read through a biometric reading?

Mr. VERDERY. If you apply for a visa now, you will go through a biometric check at the time of the visa interview and then again with US-VISIT at the port of entry to see if derogatory information has been received in the meantime or if you forged your document. And again, as of today, literally today, Visa Waiver travelers who don't have a visa are now being checked biometrically at the port of entry, at the airports and seaports.

Mr. ANDREWS. I know that it is not a totally knowable fact to know when the day will come when every port of entry has biometric reading capability, but when do you think the day will come?

Mr. VERDERY. Well, again, the most difficult one will be the smaller land ports of entry, which is by statute required by the end of 2005. These are the outposts in the middle of nowhere, so to speak. So that is the backdrop of the last date where things would be fully employed.

Mr. ANDREWS. And is that going to happen?

Mr. VERDERY. I believe it will, yes. We are committed to have the big ports of entry with that capability in secondary at the end of this year, building out in the primary lanes of entry throughout next year.

Mr. ANDREWS. So this will include by sea, by air, by land?

Mr. VERDERY. Air is complete right now for entry, and the seaports largely complete. There are a few gaps. Land this year and next.

Mr. ANDREWS. Now, let's talk a bit about biometric quality. Dr. Wein, or Wein—I am sorry if I mispronounce his name—is going to testify later this afternoon that he has concluded that a very, very small number of the readings are reliable, and he has made a suggestion that if we shift the technology for the fingerprint reading to read 10 fingers instead of what we read now, we can dramatically increase reliability, I believe, to over 90 percent from in the forties or fifties where it is now.

A, do you agree with his assessment? And B, if you do—if you don't, what is wrong with his assessment? And if you do agree with his assessment, do you think that we should make the rather modest technological change that is proposed to try to plug the hole?

Mr. VERDERY. All I have seen is his testimony for this hearing, which doesn't have the technical back-up that you might expect. I understand he has a study that will be released in the coming days, which I would expect that our team, especially the US-VISIT Office, would want to look at very carefully.

As I understand it, it is not that the majority are unreliable. It is that a small minority are unreliable if they have certain characteristics of their fingerprint. I honestly feel a little uncomfortable talking about in open session as to how to defeat the system, to be honest. But—

Mr. ANDREWS. But certainly we could generically say that there are people trying to beat the system, and there are ways to do it, right? So do you agree with his conclusion that those of—a signifi-

cant plurality, I guess, of those who try to beat the system can do so now.

Mr. VERDERY. I don't agree with that, and I don't believe our US-VISIT biometric experts do either. I don't pretend to be a biometric expert, but I don't believe they would agree with that in the way it has been presented.

Now, to go to your question you asked earlier about the 10-print. I think we do agree that in a perfect world, a 10-print solution, if it didn't take any more time and any more costs, would be preferable. But at a port of entry, at a visa issuance window, there is a big difference between putting a 10-print reader and a 2-print reader out in a primary lane or at a very crowded consular office. And so the marginal gain between 10-print and 2-print we have decided to date is not worth it because it would have held up deployment of a system that is working every day, as we speak, to find people you would not want coming into this country.

Mr. ANDREWS. I have to say I am concerned about that answer because it is my understanding that NIST looked at this study and believes that his—the professor's conclusions were conservative; that, in fact, the error rate may be higher. And remember that although the vast majority of people trying to get entrance do not in any way try to alter their fingerprint, I would assume that it is a pretty fair conclusion that a significant number of people that we are actively trying to keep out might want to alter their fingerprint. So it is a small part of the universe, but a very crucial part of the universe.

Let me also ask you this. It follows up with Mr. Gibbon's question. What mechanism is in place to move forward in biometric technology for things other than fingerprint, like eye scan? Do we have the flexibility to test those technologies, and, if so, what are we doing?

Mr. VERDERY. Well, we are actually testing the iris scan, if that is what you mean, right now in a different program, the Registered Traveler Program that TSA is operating at five airports around the country, including Reagan National, both fingerprints and iris scans, as a way to verify people who have been preenrolled in a Registered Traveler Program. And so we are working on the iris scan from that end.

As I mentioned, the facial recognition technology that will be built into international passports, will be required of Visa Waiver travelers next year. We are building in the capability to read that into our document readers at ports of entry. And so we are looking at the systems to provide redundancy and the like.

But again, the backbone of the system, from our point of view, has to be the fingerprint because that is the way our criminal records are characterized; that is how we are able to find people very quickly with very low error rates, people who should not be admitted to this country.

Mr. ANDREWS. Thank you very much.

Mr. CAMP. Thank you.

Mr. Pascrell may inquire.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. Chairman, 98 percent of over 281 million visitors annually enter our country and are inspected. That means that millions of

travelers entering the country are entering without being checked against any intelligence database that could help identify a potential terrorist or even a convicted criminal.

I am interested—when we talk about terror, General, and I want to know if you agree with me, I am talking not only about those people who wish to bring explosives into this country or to come into this country to wreak havoc on our citizens and our property, and I am talking about those people who are transporting drugs across our border. I see that terror every day in my district, throughout this Nation. And I know that drug trafficking in the United States has a lot to do with the funding and the assisting of terrorist groups and organizations. What do you see and what do you do about drug interdiction? And how do you see they are both connected?

General HUGHES. Well, thank you very much for the question. Perhaps Assistant Secretary Verdery would like to comment after I do.

Personally, I am not positive about the figures you quoted, but I grant you that there are people who successfully get into the country with drugs and who are terrorists who may come in with some capability. That certainly is true. I think it is a very small percentage compared to what it was.

We have actually been extremely successful in interdicting drug shipments, and indeed in the past 2 weeks, we have interdicted huge multiton, ship-borne movements of cocaine in the Pacific, which you may have read about in the newspapers.

Aside from that, on our land borders and in air crossings, it is pretty common for us to now interdict any kind of carrying of such material, either terrorist-related material or drug materials, through the air bridge.

The land bridge, as we mentioned, poses a significant problem for us. We are trying to do our best to control that, and there are a lot of issues there I can talk to you about, but I think we are making progress. We are on the right track.

But I don't know whether that is a good answer for you, but I will summarize it. Maritime is a huge problem, but we are being successful at interdicting, and that is often based on good intelligence. The air bridge is pretty secure comparatively for both terrorist activity involving material and narcotics trafficking. Small amounts probably arrive here and there. The land borders are an issue, and we are working hard to secure them.

Mr. PASCRELL. Mr. Verdery, would you respond to that question, please?

Mr. VERDERY. Sure. I think, as General Hughes mentioned, the numbers on drug seizures are up quite dramatically, whether it is by sea with the Coast Guard or over land at our ports of entry or the Border Patrol. We have seen no degradation of the drug mission in this Department. In fact, it has been enhanced by the additional capabilities being brought to bear. I would be happy to get you those figures on that.

We do recognize, of course, that the means by which people are able to enter the country on the land border could facilitate a terrorist looking for the same type of entry. That makes it all the more important—

Mr. PASCRELL. Well, my point—excuse me for interrupting. My point is that there is no difference in the terrorists. What is the difference? If you are bringing drugs into this country to kill our children and our citizens who are stupid enough to use it, you are—what is the difference between that kind of terrorism and the terrorism that the President has been talking about over the last 3 years? What is the difference?

Mr. VERDERY. I take the point. We want to do both. We want to fight the counternarcotics mission and also what I was referring to as more of international terrorism, which I think is a term of art.

Mr. PASCRELL. Well, would you agree with my statement that the terror of drugs in this country is just as horrible, just as terrible as the terror which is brought into this country of those who wish to bring explosives or to kill our citizens or to damage our property?

Mr. VERDERY. I wouldn't want to rank two horrible outcomes. They are both horrific.

Mr. PASCRELL. We both agree then.

Mr. VERDERY. Yes. But I think the capabilities that are being brought to bear against the terrorism threat as I define it, kind of international terrorism, Al-Qa'ida and the like, is having significant impact on the drug enforcement mission also, whether it is the One Face at the Border Initiative, getting our Customs inspectors and immigration inspectors cross-trained, enhanced Border Patrol missions, advanced technology on the border. We are seeing increases in picking up people, picking up drugs, all those kinds of things on the border.

The last point I have to make is that this demonstrates all the more reason for the President's Guest Worker Initiative, because we have got to figure out a way to get the overwhelming majority of people who are crossing the border legally, who are not criminals, who are not trafficking drugs, who are not terrorists, who want to work, we have to be able to have a way for them to walk, to come back and forth to those jobs through the ports of entry where they can be vetted for security reasons and essentially pull the wheat and the chaff, separate them. Terrorists are not going to be able to walk into a port of entry. And so if we can get the guest workers who are here to work coming back and forth through ports of entry, regularize that, it would make our border enforcement mission much better.

Mr. PASCRELL. Let me make myself clear. I didn't make myself clear then. There are 22,000 Americans that are killed every year in the United States due to illicit drugs. It would seem to me, just an observation, a perception, that we do not have the commitment to interdicting those drugs and ending this horror on the streets of our communities. And we know the tragedy of 9/11. The Commission spelled it out, made some recommendations. Some we have included in legislation conveniently, and some we have left out.

You don't have enough people to do your job. I don't care what you tell us today. You don't have enough people to do your job. So you are the messenger. I understand that. It is not you personally that I am—

Mr. VERDERY. If I could just—I mean, there is a commitment from the Department, from the Secretary, from Asa Hutchinson,

the Under Secretary, former head of the DEA, our Deputy Secretary, our operational heads such as Commissioner Bonner and our Counternarcotics Office to see this mission forward. And as General Hughes mentions, the numbers bear out that we are doing it. Are drugs getting in? Of course. This is never a 100 percent solution. But we have seen a robust increase in the amount of drugs that are interdicted in the source zone, at the ports of entry and the like, and we need to ramp it up. But we are doing the job.

Mr. PASCRELL. I just wanted to bring something to your attention, that is, on the Border Patrol. We are talking about, in 2011, there were 9,700, almost 9,800 Border Patrol. There are 10,839 today. How can you sit there and tell this committee—being the messengers, how can you sit there and tell this committee that by adding the small amount of Border Patrol, that you are even touching the surface of this serious problem.

You know that there are more drugs coming into this country than ever in the history of the Nation. You don't have enough people to do the job. We are doing this on the cheap, and we are doing this for what the reason?

I don't know why we are holding this hearing today, I really don't. We need to act and we need to act yesterday. And that was the whole message of the 9/11 Commission, we need to act yesterday. And we need to do it in a very tangible way, rather than simply having committee upon committee, everybody gets a piece of this, and nothing is being done.

There is terror in our streets, and there is terror from drugs in this country that are moving freely. You know it and I know it. Just as serious as the lunatics that are out to try to kill us—just as serious.

Mr. CAMP. Thank you. The gentleman's time has expired.

And before I recognize Mrs. Lowey, the purpose of this hearing is to look at terrorist travel. We have separate committees in this House that deal with narcotics, and there are some Members that are on both committees, like Chairman Souder who has done a great deal of work in this area.

So I appreciate the gentleman's line of questioning, but this hearing, in fairness to our witnesses, is about terrorist travel. And I realize—

Mr. PASCRELL. I am talking about terrorist travel, Mr. Chairman.

Mr. CAMP. I realize, by your definition, but we have separate committees—

Mr. PASCRELL. That is why I asked the question.

Mr. CAMP. But we have separate areas that are also working on this.

So, with that, I would recognize the gentlewoman from New York, Mrs. Lowey, to inquire.

Mrs. LOWEY. Thank you, Mr. Chairman.

Gentlemen, good to see you again. Tuesday's New York Times reported, based on the findings of an FBI inspector general report, that 3 years after the September 11th attacks, more than 120,000 hours of potentially valuable terrorism-related recordings have not yet been translated by linguists at the FBI.

My judgment, this is absolutely outrageous, not to mention dangerous, particularly for the residents of my home State of New

York which is referenced in intelligence reports time and time again.

In my judgment, we can collect all of the intelligence we want, but if we let it sit on a shelf and collect dust for 3 years, it won't do us any good. We are here today, in part, to review the progress being made by the Department in the area of information sharing.

And perhaps, Secretary Hughes, could you just tell me what this report indicates to you, and what you are doing about it?

General HUGHES. It indicates to me that we—and actually I guess I will use a little bit of history here—we haven't solved the problem we have had for many years, where similar kind of records have been found throughout the intelligence community, not just at the FBI, but at the National Security Agency, the Central Intelligence Agency and the former office that I held, the Defense Intelligence Agency. We are overwhelmed, in fact, many times by the volume of material.

We do have some screening mechanisms to go through this material and highlight to us the issues of interest that are in them, rapidly, key word search, as an example of anything that can be digitized. That is not the only—

Mrs. LOWEY. Secretary Hughes, if I may, but I know that my time is fast disappearing. You are the Assistant Secretary, Information and Analysis. I may not get to my next question about border security. But it is 3 years after 9/11.

I have three children, I have seven grandchildren; I want to know what you or others who have similar responsibilities are doing about this now? This is an embarrassment. It should be an embarrassment to you, to Secretary Ridge, to the FBI. What are we doing about it now?

General HUGHES. I don't think I can answer your question. I don't know what we are doing about it now, outside of being equally outraged, as you are, about the report. I don't actually know if the report is completely accurate.

But let's assume that it is for a minute. What I intend to do is to ask questions about it in the appropriate forum and to seek full detail, and then search for ways to solve this problem. I am sorry if it seems like I was talking on anything something that wasn't related. But, indeed, it is related, ma'am.

We have had these problems for 20 years or more. And we are likely to have them in the future. The volume of information and the number of people to deal with it is in great imbalance.

I apologize for giving you that answer.

Mrs. LOWEY. No, I appreciate your honesty, sir. But I just want to say, as someone who sits on Appropriations, I know the—in addition to this committee, I know the billions that we are spending. We spent billions organizing this Department of Homeland Security.

I had real concerns that instead of dealing with issues like this and replacing incompetent people with competent people, we have been moving chairs around. Some people aren't even in their offices yet. So I just wanted to send a very strong message that if my first responders—my police, my fire fighters—are going to be getting plans in place to deal with emergencies and the FBI doesn't even have all of these urgent messages interpreted—as you know, before

9/11, part of the problem was they couldn't get the messages to the right people; and I am not even talking about other issues that our first responders have. But if we can't get these messages interpreted in a timely way, we might as well just all say, Give up, save the money, put it into our schools, put it into our health care, the Department of Homeland Security is just not doing what it should.

And I hate to be so strong, because I know you are working so hard. But I just hope that if I am sending my strong message to you, it is gotten, and you can report back to me and to the committee as soon as possible with a plan that is going to address this.

Mrs. LOWEY. I don't know if we are going to have a chance to ask other questions, but Solomon Ortiz, my colleague, has been asking a lot of question about the gangs, the illegal immigrants that have been coming over the border. Unfortunately, the head of counterintelligence at the CIA, never heard about that.

So I hope, Mr. Chairman, you all have heard about it. He didn't know about it, and so there seems to be a real problem of people in one office not communicating with people in other offices. And I hope, Mr. Chairman, if we have another round, we can deal with that, because that is truly a major issue in border security. Thank you.

General HUGHES. May I give one brief answer?

One of our—

Mrs. LOWEY. I am talking about the catch-and-release issue.

General HUGHES. I understand—and the gangs. My point that I was going to make is, one of our primary databases is called VGTOF it is the Violent Gangs and Terrorist Activities or Terrorist Organizations Database.

We combine the two in at least one database and look at them with equal vigor for lots of reasons. And part of the reason is, we believe, I strongly believe, there is a connection. So MS13 from El Salvador or Honduras here in the United States and Al-Qa'ida somewhere else, I believe does have a relationship that is important for us to understand.

May I just close by saying, I share your passion, and I will do my best, ma'am.

Mrs. LOWEY. Mr. Chairman, I think it is just important to remember, and I know if we get to another round, that the problem here is that these illegal immigrants are released under their own recognizance.

And I have a feeling that they might not all be home just knitting with their families or cooking dinner. And I think it is an amazing issue that many of my colleagues have spent a lot more time focusing on, and I was just going to bring it up today.

Thank you, Mr. Chairman.

Mr. CAMP. Thank you.

Mr. Langevin.

Mr. VERDERY. If I can have a brief minute to respond. But you mentioned that there were catch and release. That is obviously a concern of ours, because there is an imbalance between the number of people who are picked up, who are scheduled for deportation, and the amount of beds we have.

Now, within that imbalance, ICE has gone to great lengths to prioritize people who have been found to be involved with criminal

activity, violent criminal activity, or are non-Mexican. So we are trying to prioritize amongst our bed space to keep the violent felons in custody until they are deported, as well as trying to improve the deportation system itself to get more people through the system, whether it is through repatriation, getting people back to countries that won't take them.

We are trying to move more people through so we have less catch and release.

Mrs. LOWEY. Maybe you should have more bed space.

But, Mr. Chairman, I won't take any more time.

Mr. CAMP. Thank you.

Mr. Langevin may inquire.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Gentlemen, thank you for being here today. Andrews, who is clearly on the same wavelength addressed my question in large part, but I do want to follow on, if I could, and just explore a little further where we are, how close we are in terms of having a robust system that is as close as possible to 100 percent effective when it comes to biometric scanning of fingerprints.

What are you doing to get us to that 100 percent level, and in terms of a time frame, at what point can you give assurance to the public that we are as close as we are going to get, that it is a 100 percent accurate scanning system?

Mr. VERDERY. Well, if you think of—

Mr. LANGEVIN. If I could, in addition to that, are we giving equal attention in terms of the technology that is deployed to airports, ports of entry and land border crossings, particularly in light of the fact that there are some that suggest that Al-Qa'ida would prefer a port of entry as opposed to some of the other methods coming in?

Mr. VERDERY. Well, thank you for that question, sir.

Again, VISIT is being deployed in fairly well-identified, discrete increments: Increment 1, January 5 of this year, airports and seaports. It is now 100 percent at airports, so every international traveler, with the exception of diplomats and a couple of other minor categories, basically 100 percent are vetted biometrically at the port of entry, at airports.

Seaports are close to 100 percent for entry. Land borders, we will put US-VISIT capabilities in secondary processing by the end of this year at the 50 biggest ports, the very heavily trafficked ones, and at the smaller ports of entry by the end of next year, by 12/31/05.

The VISIT capability on primary, because essentially when your cars are driving through you are talking about primary, will be deployed throughout 2005 at the big ports of entry and 2006 for the smaller ports of entry.

In terms of how are we deploying it, we recognize there is no way to make everyone get out of a car at primary, with literally millions of people coming through. So we are going to be going with a radio frequency technology solution, so that the biometric information is pulled off your travel document as you are going through the port of entry ahead of time, so that the inspector can see the information, see if there is a potential problem while there is still time for a law enforcement response or other necessary action. And that

same solution will be deployed on exit, so there is an exit at the port of entry, as well as for land.

I think I mentioned the airport exit solutions will be deployed this year, and throughout next year there will be a universal airport and seaport exit.

So I think the bottom line for airports and seaports, you are looking at near 100 percent coverage by the end of next year; land ports, 2006.

Mr. LANGEVIN. What about the accuracy of the technology itself? As Mr. Andrews was—brought up, Dr. Professor Wein's findings indicate that the technology itself in some cases may be as low as 52 or –3 percent in terms of its accuracy. You feel it is higher.

But, clearly, it is not at 100 percent. So what steps are you taking to get us as close to 100 percent accuracy as possible? And how long before you have confidence that it is 100 percent accurate when the technology is used?

Mr. VERDERY. Well, what we found in the 9 million or so people who have been enrolled in US-VISIT this year is that the accuracy is quite high. The false positive rate is less than 1 percent. And those people are resolved usually very quickly, in a couple of minutes in secondary, where a fingerprint appears to be a match against a watch-list, but is not. There also are small numbers of individuals whose fingerprints cannot be taken for medical reasons or other reasons.

The issue that was raised by the witness in the second panel is, I think, a little bit different than that. It is a question of, if you are trying to defeat it, how easy is it to essentially try to rig the system. And again I don't feel real comfortable talking about that in open session. I would be happy to come in and talk to you privately about that.

But in terms of the overwhelming majority of individuals, it is working extremely well, in the 99 percent range.

Mr. LANGEVIN. My time is almost up, so quickly I would like to ask this.

I still am constantly baffled by the sheer number of different databases and lists available for determining who requires extra screening and who should or should not be flying. And I can't believe that we still don't have one complete and integrated list that can be effectively used for our Border and Transportation Security infrastructure to thwart terrorist travel.

So can you provide some more detail as to what your goal is in terms of streamlining those lists and ensuring that they are used effectively? And can you tell me exactly when that goal will be met?

Mr. VERDERY. Well, the watch-listing effort is being led by the Terrorist Screening Center established by the President last year. The terror screening database is what is accessed by our frontline people, whether it is the TSA screener or an airline in terms of enforcing the ″no-fly″ list. So essentially we do have a common set of watch-lists that are now used, depending on the program.

So the problem we have, and the reason you see these stories in the paper of people being flagged inappropriately, and the like, is not so much a problem with the list, it is a problem with the implementation of the list. Right now, it is being run by each of 77 dif-

ferent airlines differently. Essentially, your person that is checking you in is essentially acting as the watch-list enforcement person.

We recognize that is not a tenable solution. That is why we have proposed a Secure Flight program to bring that responsibility within the government's sphere, within the TSA. But to do that, we have to get information from the passenger, via the airlines, in time to make that determination.

So we have issued an order to compel data for testing of the system. That will be followed on by an order compelling data to make the system go live, so that we can handle this and leave airlines with the responsibility of trying to enforce these lists. It will be based on the Terrorist Screening Center's coordinated watch-list.

Mr. LANGEVIN. Can you give a time frame? Can you assure the public out there that we are not going to see these kinds of stories in the paper where we have got different lists that don't pick up accurately the people that should not be flying?

Mr. VERDERY. Secure Flight, I believe, is due to become operational in the spring, post-testing; that is when you will see the transition from the airline-based system to the government-based system.

Will it be 100 percent? No. Because there are so many air travelers, there will be false hits. If we have somebody on our watch-list whose name is Bill Jones, there will be other people named Bill Jones who are flying, and we have to resolve those types of potential hits.

I am always amazed at how many similar names there are, when they sound like a common name; but you put the entire American people and our international travelers out there flying, you are going to have those types of hits that have to be resolved. That is why we are working on Secure Flight.

Mr. CAMP. Thank you.

The ranking member of the full committee, Mr. Turner, is recognized, if he would like to inquire.

Mr. TURNER. Thank you, Mr. Chairman.

I think the first thing I would like to talk about is this problem we have on the border with the catch-and-release practice that is ongoing. Do we have a figure available, Secretary Verdery, that would tell us what it would cost us to end that practice?

Mr. VERDERY. A figure on how much it would cost to detain every person who is apprehended until they are deported?

Mr. TURNER. Yes.

Mr. VERDERY. I do not have that in front of me. It would be quite large.

Mr. TURNER. Has there been any consideration of some temporary detention facilities that would enable us to halt that practice?

Mr. VERDERY. Well, there are temporary facilities used on occasion. That is what we have done in Arizona where we have gone in and enhanced the resources.

We recognize there has to always be a balance of the prosecutorial resources, the detention resources, the removal resources. And if you end up with an imbalance, you essentially haven't done any good, because you can't get people through the system appropriately.

So there has to be essentially a continuum. So, in that case, we have put more temporary space in Arizona.

Mr. TURNER. I am told by some of the Border Patrol people that I visit with that the catch-and-release practice fairly quickly has become well known among those who are engaged in human smuggling. And so we are likely to have seen an increase in efforts to come across our unprotected borders as a result of the fact that it has become known that if you are from a place other than Mexico, you have about a 50 percent chance of being released on your own personal bond if you come into our country.

And I would suspect that we could at least make some impact upon the movement of illegal immigrants from places other than Mexico if we had some effort—made some effort to try to stop that practice.

Mr. VERDERY. Well, regarding the announcement that we had recently of the new use of expedited removal, it points out the need for that. It essentially is going to say, if you are from a country other than Mexico and picked up between a port of entry and you do not have an asylum claim, you are going to be held, whether it is a couple of days, a short period of time. You are going to be flown back, you are not going to be put into the system taking up a bed for months, even years. We can move people through more quickly.

Again, I have our detention numbers: 108,000 in 2001, 113,000 in 2002, 145,000 in 2003. We had 130,000 in 2004 through June, so I think we are on track to have quite a bit of increase from last year. But, again, there is no shortage of people in this regard.

Mr. TURNER. The Border Patrol people that I visit with say that they have received no instruction from the Department regarding how this new expedited deportation process is going to work, no indication of what kind of training the Border Patrol agents will be receiving, no indication of when this is going to be implemented.

We have a program here that you have announced, but there doesn't seem to be much understanding among the rank and file about how it is going to work or where you are getting the money to pay for it. Could you help enlighten us on that?

Mr. VERDERY. Well, it is operational in two sectors, in Tucson in Arizona and Laredo in Texas. So if you are not a Border Patrol agent in those two sectors, then you probably wouldn't have been trained, because it is not being applied. In these sectors, training has been completed. I have to get back to you on exactly how many people, but the training has been provided.

There was a month lag time between the announcement and when it became operational, so they can get their proper training, to make sure we are abiding by our asylum requirements under international law.

In terms of the funding, this is a money saver in the long haul. It is going to move more people through, and will be a deterrent effect against the migrant flow that you mentioned.

And if I might just mention one other thing while I have the floor, a very important announcement from last week is that we have now integrated at the Border Patrol stations the IDENT and IAFIS fingerprint systems, which were formerly separate systems developed by the Justice Department. We have integrated work

stations available at all Border Patrol stations so that if Border Patrol picks somebody up, they can not only check it in IDENT, which has information about prior illegal crossings and immigration information, but also against IAFIS, which has all of the criminal database from FBI and other sources.

So we will have an end to that situation where people were picked up for a crime in one State, and then Border Patrol didn't know about it. We have already had a number of successes of violent criminals being found. Of course, that means those are the types of people we are going to detain. They are not going to be part of a catch-and-release policy, so to speak, but will be the priority people that will take up those beds.

Mr. TURNER. Do you have the capability to access the FBI database to know who they may have on their database when people come to Border Patrol stations?

Mr. VERDERY. That is exactly what I was just talking about; the IAFIS system is what FBI operates. So, yes, if Border Patrol picks somebody up, they are now run against IAFIS to see if there is a prior criminal record. we had promised that was going to be deployed in 70 percent of the Border Patrol stations by the end of this year, and we will have beaten that by going to 100 percent as of last week.

Mr. TURNER. Do you feed information back to the FBI regarding people that you picked up? do you feed records into the same database that you receive information from?

Mr. VERDERY. They have access to IDENT through the US-VISIT program. And we have actually just announced an enhanced access by FBI to do searching through IDENT, whether it is the Border Patrol information you mentioned, or the entry-exit information through US-VISIT. They do have access to that. We are enhancing that.

Mr. CAMP. Thank you. The gentleman's time has expired.

We have another panelist that we would like to hear from.

I want to thank both General Hughes and Assistant Secretary Verdery for being here this afternoon. And this would conclude your testimony before this subcommittee today. Thanks again for being here.

Mr. CAMP. The next panel will include Professor Wein. I want to thank Professor Wein for coming all of the way from California to testify at this hearing. Professor Wein can come and take a seat at the table. Thank you.

We have your written testimony. If you could briefly summarize your statement in 5 minutes.

STATEMENT OF PROFESSOR LAWRENCE M. WEIN, GRADUATE SCHOOL OF BUSINESS, STANFORD UNIVERSITY

Mr. WEIN. Good afternoon, Chairmen Camp and Gibbons, Ranking Member Turner and members of the House Select Committee on Homeland Security. I am honored to appear before you today to discuss a serious but repairable vulnerability in the biometric identification performance of the US-VISIT program.

The implications of our findings are disturbing enough that last week I briefed members of the Homeland Security Committee, staff from the Office of the Vice President, and analysts at the General

Accounting Office, and program managers at the US-VISIT program.

On the surface, the biometric identification of the US-VISIT program appears to be highly effective. A NIST May 2004 report estimates that the chances that a terrorist who is on the watch-list—when entering a port of entry, the chances that we catch them and have a watch-list hit is 96 percent, while maintaining a false positive rate, that is the probability that someone like you or me would nonetheless set off a watch-list hit, maintaining that probability at a mere 3 in 1,000.

So what is the problem? Well, the devil is in the details. It turns out that the software systems also report and determine the quality of each image. And the software has a very difficult time in accurately matching images that have poor quality.

And the premise of our study is that terrorist organizations, such as Al-Qa'ida, will exploit this vulnerability by choosing U.S.-bound terrorists who have inherently poor image quality, such as worn-out fingers or deliberately reduced image quality. Why is this?

First, all of the information is public; it is on the NIST database; two, Al-Qa'ida has a large pool of terrorists from which to choose; and three, we know they are sophisticated enough. Indeed, given the intricacies of the planning of the 9/11 attacks, I think our assumption is not only prudent but realistic.

So using publicly available information from the NIST Web site, we developed and analyzed a new mathematical model that includes red-teaming. First, the U.S. Government chooses a biometric strategy, essentially the rules that decide how you determine if a watch-list hit happens. So they choose a strategy to maximize the chances of catching a terrorist, subject to maintaining moderate congestion at the ports of entry under current staffing levels.

Then the terrorist tries to defeat this system by choosing his or her own image quality to minimize his or her chances of getting caught. And the results are sobering. The currently implemented strategy has only a 53 percent chance of detecting a terrorist at U.S. points of entry, compared to the overall level reported in the NIST report of 96 percent.

Again, the deterioration, down to a coin flip here, is due to the fact that the terrorist is allowed to exploit the vulnerability in the biometric system.

We have two main results. The first result is that instead of using a one-size-fits-all decision rule for who gets a watch-list hit, we derived different rules for different image qualities. And by doing so, we were able to increase the detection probability from 53 percent to 73 percent. So from essentially a coin flip, up to almost three-quarters. This is a minor software fix.

Over the next few days, I will give a detailed mathematical paper to people at NIST, to people at the US-VISIT office, and this should be implemented as soon as possible.

Now, even if we increased inspector staffing levels significantly, we can't really get over the three-quarters level, over the 75 percent chance. But now here is our second result. If we take 10 fingers at visa enrollment, and then have the opportunity at ports of entry to use more than two fingers for the people with the poor

image quality, then we can increase our detection probability all of the way up to 95 percent without increasing the false positive rate.

Although switching from a two-fingerprint to a 10-fingerprint system may be costly and certainly would be disruptive, there is simply no excuse for a $10 billion program to not achieve a 95 percent performance level, particularly given the potentially grave consequences of allowing a detection—allowing someone, a terrorist, to cross the border.

If slower two-finger matching algorithms cannot in the immediate future approach this 95 percent detection probability for poor quality images, then the US-VISIT program should be reconfigured with 10-fingerprint scanners as soon as possible.

Thank you. And I look forward to taking your questions.

[The statement of Mr. Wein follows:]

PREPARED STATEMENT OF LAWRENCE M. WEIN

Good afternoon, Chairman Cox, Ranking Member Turner, and the Members of the House Select Committee on Homeland Security. I am honored to appear before you today.

I am the Paul E. Holden Professor of Management Science at the Graduate School of Business, Stanford University. I teach operations management to MBA students, and perform research in the areas of operations management, medicine and biology. At their essence, many homeland security problems are service operations problems: Just as McDonalds needs to deliver hamburgers in a rapid and defect-free manner, the US Government needs to quickly deliver vaccines and antibiotics after an attack and to safely prevent nuclear weapons and terrorists crossing our borders.

Since September 11, 2001, I have used mathematics to analyze a variety of homeland security problems in bioterrorism (effective responses to terrorist attacks using smallpox, anthrax or botulinum toxin) and in border security (evaluating ways to detect nuclear weapons coming through ports). These analyses have led to policy recommendations, several of which the U.S. Government has adopted.

Today, I am here to discuss the results of a study I conducted at Stanford University with Ph.D. student Manas Baveja that examined the ability of the US-VISIT program to accurately match the fingerprints of visitors at ports of entry against a watchlist that contains the stored fingerprint images of suspected terrorists. The implications of our findings are disturbing, so much so that last week I briefed members of the Homeland Security Council, staff members from the Office of the Vice President, analysts from the Government Accounting Office (GAO) and officials from the Department of Homeland Security.

On the surface, biometric identification of the US-VISIT Program appears to be highly effective. A May 2004 NIST study, entitled "Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints," predicted that the likelihood that US-VISIT would flag a terrorist whose fingerprints are stored on the biometric watchlist is 96%, while simultaneously limiting the false positive probability, i.e., the likelihood that a visitor not on the watchlist would nonetheless generate a watchlist hit, to 3 in 1,000.

So what's the problem? It turns out that the devil is in the details: The biometric software also computes the quality of each fingerprint image, and it is very difficult to accurately match poor-quality images. Our study stems from the belief that terrorist organizations can exploit this observation by choosing US-bound terrorists that have either poor image quality (e.g., worn out fingers) or deliberately reduced image quality (e.g., surgery, chemicals, sandpaper). The relevant data is publicly available on the NIST web site, and we know Al-Qa'ida has the sophistication to understand this and has a large pool of potential terrorists to draw from.

Using publicly available biometric data from NIST, we developed and analyzed a novel mathematical model that allows red-teaming: First, the government develops a biometric strategy to maximize terrorist detection for a given inspector staffing level, and then the visiting terrorist attempts to defeat the biometric system by choosing the image quality to minimize his chances of getting caught.

The results are sobering: the currently implemented strategy has only a 53% chance of detecting a terrorist during US entry, compared to the overall value of 96% mentioned earlier. The detection probability is reduced to essentially a coin-flip because the terrorist is allowed to exploit the vulnerability in the biometric system.

The good news is that our study pointed to possible solutions that our nation can implement. Rather than using the current one-size-fits-all rule for generating watchlist hits, we derived different rules for different levels of image quality and improved the likelihood of detecting a terrorist from 53% to 73% without increasing the false positive rate.

Unfortunately, our study predicts that increasing staffing levels of US Custom and Border Protection inspectors would offer only modest benefits, and could increase the 73% detection by only an additional 5%. Given that US-VISIT runs millions of watchlist checks each year, this is an unacceptable security risk.

Fortunately, our nation has a second solution it can rely upon. Instead of using a software system that scans two index fingers, we found that that allowing additional fingers to be tested from people with worse image qualities achieves a 95% detection probability, without increasing the primary plus secondary inspection workload associated with legal visitors.

Finally, the government's investment in biometrics at ports of entry for detecting terrorists should be assessed in light of the detection probability required to deter terrorists from crossing at an official port of entry. The deterrence value of a fingerprint system depends on the terrorists' perceived likelihood of successfully entering the US between the ports of entry, e.g., along the US-Mexico border. While this detection rate has been estimated to be approximately 25% in a recent Time Magazine article, it appears that Al-Qa'ida prefers to enter the US at ports of entry.

To summarize, there is a serious but reparable vulnerability in the biometric identification system of the US-VISIT Program, which is our last line of defense for keeping terrorists off U.S. soil. A minor software modification that allows the watchlist rule to vary with image quality can increase detection from 53% to 73%. I have provided details to officials who oversee the US-VISIT operations, and this should be implemented as soon as possible. The use of more than 2 fingers for low-quality images can achieve a detection probability of 95%. Although switching from a 2-fingerprint to a 10-fingerprint system may be costly and disruptive, there is no excuse for a 10-billion dollar program to settle for performance below this level. Indeed, our results are not inconsistent with the warning in the November, 2002 NIST report that a 2-finger search was not sufficient for identification from a large watchlist. If slower 2-finger matching algorithms cannot approach 95% detection for poor-quality images, then the US-VISIT Program should be reconfigured with 10-fingerprint scanners as soon as possible.

Our recommendations hinge on the assumption that terrorist organizations as sophisticated as Al-Qa'ida will eventually attempt to defeat the US-VISIT system by employing terrorists with poor-quality fingerprints. In light of the meticulous planning that went into the 9/11 attacks, I believe this assumption is not only prudent, but realistic.

Thank you, and I look forward to responding to your questions.

Mr. CAMP. Thank you very much. We just had, last week, a demonstration of some of the technology available in biometrics, and they didn't have exactly the same rates.

I think the way you look at your data is a little different than theirs. But I understand your concern is that people intentionally deface their fingerprints and then—on a two-finger scan system, that is not that hard to do, and they will circumvent.

Now, in theory, if there is a bad read or an inability to read a fingerprint, there should be diversion to secondary screening at that point under the system. But my question is more about alternative biometrics.

I have seen some demonstrations on facial scans. I am not sure that 10 fingers is really the best direction that we should go. It is almost landline versus wireless in terms of telecommunications. But it seems to me that this facial reading has a much higher rate of accuracy, which is in sort of the development stage.

As you referred to, there are other biometrics, such as eye scans. Can you comment on those and give us some information on what you—

Mr. WEIN. Yes. The operative word you bring up is "development." These are in the development phases. I have worked on port

security also with Stephen Flynn on some of these issues. It is a hard problem, because you have all of this technology that may provide a silver bullet, but it may take 5 or 6 years. But the terrorists aren't going to wait 5 or 6 years to sneak a nuclear weapon into the country.

NIST has done quite a bit of analysis on face biometrics, and they claim for large-scale identification of the size we are talking about here, it simply is not a feasible option. The iris and eyes—I have read up on all of these, and some of them sound promising; they may be ready in several years, they are not ready for prime time. Either they have too many false positives, people don't like to have various parts of their eye scanned and so forth. So, whereas, it may not be viewed as wireless technology, taking 10 fingers clearly will help a lot.

Indeed, my recommendations are not inconsistent with what is reported from the NIST way back to November of 2002, that two-finger methodology is simply not adequate to do large-scale identification.

Mr. CAMP. Well, it seems if you could deface—

Mr. DICKS. Would you yield just for a second?

I think you were here. We had a meeting here, and they came up and told us that two fingers gave us 95 percent reliability.

And you are saying that is not true, because there are quality problems associated with two fingers or any fingers, and that is why you should do 10, in order to get the higher reliability; is that not correct?

Mr. WEIN. The 95 percent is averaged over the entire population. The overwhelming amount of the average population, like you and me, we are not attempting to defeat the system.

Part of the reason we are putting this program in place is to stop terrorists from coming into the country. It would be naive to think that these people are not trying to defeat the system.

An insignificant fraction of people have naturally worn-out fingers, have naturally poor image quality. It is on the order of 5 to 10 percent.

Mr. CAMP. If I could reclaim my time, my point was, we did have a higher number. I think he is looking at it a little differently.

But, second, if you can deface two fingers, you can deface 10, and we ought to be looking at other means—my point is that.

US-VISIT is just one of the items that we have to try to disrupt terrorist travel. We also have, you know, this other biometric capability. We have the watch-lists that we just had an extensive discussion on. There are inspectorinterviews. There is secondary screening. There is actual real intelligence that has helped disrupt this.

So this is just one of the many items that we are looking at in terms of how we disrupt terrorist travel.

Mr. WEIN. I think it is important on many of these homeland security problems to move forward in two ways. One is, operationally we need to get things in place that are effective, and get them in there quickly, because Al-Qa'ida and other terrorist organizations are not going to wait.

And second, we need to keep an eye towards the future of trying to find better technologies, be they biosensors, be they radiation detectors, be they biometrics, to help us on the 5-to–10-year time line.

Mr. CAMP. The last point is that the additional fingerprints, from what we understand now, would take a great deal of additional time. To get in this 45-second or 50-second window at the booth is very important in terms of not disrupting travel for those citizens who are not trying to do us harm. So it is a balance there.

Mr. WEIN. My analysis is conservative. I am assuming each finger takes 5 seconds. So if you did 10 fingers, it is going to take you 50 seconds rather than 10 seconds that it currently does.

Mr. CAMP. Well, it takes longer than 10 seconds with two fingers, because of the entire process. But I understand your point.

Mr. WEIN. Right.

Mr. CAMP. We are not there yet in terms of speed.

Mr. WEIN. Right. But, MITRETEK and NIST and have proposed the four-finger slap. And, indeed, they think they can do this quite quickly, more like doing it in 10 seconds rather than in 50 seconds. And, indeed, I have been told ergonomically that you can actually get better prints from the slap, because your fingers are more stable.

Mr. CAMP. Thank you. My time has expired.

And I would at this time recognize the ranking member of the Border and Infrastructure Subcommittee, Ms. Sanchez, to inquire.

Ms. SANCHEZ. Thank you, Mr. Chairman.

And thank you, Professor. I am trying to understand what you were telling us.

Are you saying that over a large range of people, an end sample being almost infinite, or 200 million, or whatever we have in the United States, that if we look at all of our fingerprints, we have a 95 percent good match, but if we are taking a look at a much smaller number, these people who we think are terrorists or would happen to be on a list, that because we think that they might deform their fingers in some way or something, that the percentage would therefore be lower?

I am trying to understand how you get down to the 50 percent.

Mr. WEIN. Right. The 95 percent that they give us is over everyone. But it turns out, on the order of 5 percent, let's just say, people have poor image quality.

For the most part, this is naturally poor image quality, people who have worn-out fingers either genetically, or they have scrubbed floors all of their life or whatever. Al-Qa'ida has a large pool of terrorists to choose from to come into this country. There are pictures on the NIST Web site of what a low-image-quality finger looked like.

Ms. SANCHEZ. So they can select those people who they think are low-image people to put into the pool of people we would be concerned about?

Mr. WEIN. Right. So they don't even have to deliberately deface their fingers with sandpaper or chemicals or surgery or whatnot. They can simply choose people for their U.S.-bound missions who have poor image quality.

Ms. SANCHEZ. You said, if we took these 10 fingers at the visa processing—when we were processing the visa, that it would take about a minute a person?

Mr. WEIN. Well, we would take the 10 fingers at enrollment, so we have the 10 fingers. We wouldn't need to use all 10 fingers, except for the people with bad image quality. We would have that information when they show up at port of entry, Oh, this is a person who has bad image quality. We are going to use 8 or 10 fingers here at the port of entry.

What you can do at port of entry is take 10 fingers from everyone, so that everything else can be blind to both the operator and to the visitor of how many fingers you use to actually try to figure out if they are on the watch-list.

Ms. SANCHEZ. OK. I just wanted that clear for my own information. Thank you, Professor.

I will yield back my time.

Mr. CAMP. Thank you.

Mr. Gibbons may inquire.

Mr. GIBBONS. Thank you, Mr. Chairman.

Mr. Wein, thank you for being here. Appreciate your testimony. As you know, the State of Nevada for many years has had biometrics within their gaming industry that uses massive, large-scale recognition of large crowds to be able to single out a selected individual based on facial recognition features. And I am sure that their system, while not perfect, could be an ancillary or additional check for a person coming through either the screening at a port or, at the same time—

But let me ask a completely different question that goes to this quality image that we talked about. How much of the quality is outside of the control of the Department of Homeland Security? I mean, you talked about the characteristics of the fingerprint,but is there a quality issue with the machine, a quality issue with the training, a quality issue with the software?

How much of it is outside of their control, and therefore, what portion could be corrected by going back and doing, like you said, software versus the quality image of having a bad series of fingerprints?

Mr. WEIN. That is a very good question. We asked ourselves that in the process of this research.

Unfortunately, the available data from NIST doesn't exactly answer that question. But we do have an analysis that is quite technical—I won't go into it now—but it suggests that the great majority of this is inherent in the fingers and is not operational noise due to sweat and dirt and finger pressure and things like that.

I do think it is important to train the operators to keep the operational noise or environmental noise as small as possible by, you know, cleaning the fingers and cleaning the surfaces where they are putting the fingers and making sure they are holding their fingers steady and things like that.

In talking with the US-VISIT people last week, it sounds as if good operations processes are in place. So I think US-VISIT is doing all they can on the image quality problem—I mean on—in reducing, on getting rid of the operational noise. And most of it is

simply inherent in the people; that is why we really need to make these fixes I recommended.

Mr. GIBBONS. OK. Let me go back to the issue of other biometrics, particularly facial recognition. Is facial recognition enhanceable by increasing the number of points on a face from today's standard—I guess what is it, 14 or something like that?

What if the facial recognition capability were 200 points on a given picture of a given face? Is the likelihood or accuracy of that biometric far greater?

Mr. WEIN. I can just tell you that my analysis, and what I will distribute in the next few days to the government, cites a paper from NIST that says for large-scale identifications, that is, one-to-many matching for a large watch-list, facial biometrics is inadequate to even help on the problem. It just isn't feasible at this point in time.

Mr. GIBBONS. Do you know why they say that?

Mr. WEIN. The data is there. I would have to go back and look at the paper to give the reasons. They mostly do a statistical analysis, look at this, and conclude that the facial recognition cannot help. It certainly is great for verification one-on-one, are you who you say you are, but when you are comparing it to all of the millions of people on a watch-list, it is simply—

Mr. GIBBONS. Is it because of the computer technology where we have to sort through a large, massive database in order to have sufficient evidence, or time or recognition features that would allow for a more accurate determination of who the individual is with something like that?

Mr. WEIN. As I understand it from reading, there is a lot more noise involved in taking someone's picture, the lighting, the shadows, the angle, things like that, than there is on a finger. That is why there are many more false positives.

And when you start thinking about a false positive, when you are comparing against hundreds of millions of people, you are getting back to the John Doe that the assistant secretary was talking about. There are just too many John Doe's on the watch-list.

Mr. GIBBONS. It just seems to me that if we can control the quality of the fingerprint, we can control the quality of the photograph.

Mr. CAMP. Would the gentleman yield?

With the new facial recognition, the lighting is not as important as in past times. So there is some new technology there that really gets around that problem.

Mr. GIBBONS. Mr. Chairman, my time is up.

Mr. WEIN. NIST has decided—has said that facial recognition has gotten much better in the last few years, but it still cannot help on the problem of large-scale identification. Maybe in 5 years, hopefully, but not now.

Mr. CAMP. The gentleman from Texas, the ranking member of the full committee may inquire.

Mr. TURNER. Thank you, Mr. Chairman.

Professor, the NIST scientists that our staff has talked to say that, if anything, your numbers are very conservative, that the quality of the fingerprint images in the terrorist watch-list is even worse than what you are talking about.

So it seems to me that you are telling us something that is very, very troublesome. And I don't know how much worse they think it can be than your 50 or 52 percent number.

Did they give you any indication? Have you talked to them about what they think about this?

Mr. WEIN. I only talked to one person from NIST who was present when I briefed the program managers from US-VISIT last week.

It is true that NIST has said over and over again in their papers, which are publicly available on the Web site, that the test databases they use, in some sense are much cleaner than the true operational databases that we are using to try to catch terrorists. And, indeed, there is going to be lower image quality in general on the real databases than there is on these test databases.

Obviously, at this point in time, they are not sharing those numbers with me, so I can't say what the magnitude of that is. But I would agree with their assessment that my numbers are conservative and are painting, if anything, an optimistic view of the current operation.

Mr. TURNER. I mean, this is quite disturbing. We are talking about a program that was announced and estimated to potentially cost the taxpayers $10 billion to put in place. And you are saying, even by your numbers, the chances of catching a determined terrorist may be only 52 percent.

Mr. WEIN. Yes. And, you know, one good thing is that a chunk of that, you can get maybe from 50 to, 70 or in real terms, maybe 40 to 60 or whatever by just a few lines of software code. So that is part of the silver lining here.

But, yes, I do want to just reiterate that a program this expensive and this important with the implications of allowing terrorists into this country, given that there is an existing fix that we can do that doesn't involve—well, it does involve some retrofit—I realize there are space constraints at the ports of entry. But this seems like a no-brainer, that we have the 10 fingers available, we can get it, and let's do it.

Mr. TURNER. And so that fix, moving to 10 fingers and changing the software, would move it up to where we might have a 75 percent chance of catching a terrorist that was determined—

Mr. WEIN. Yeah. I think that is conservative. I would think it would be higher than that.

But, again, one would really have to almost, you know, look at the true database, and probably people with security clearances—and I don't know if it is NIST or people at the US-VISIT—would have to run the final numbers. But I think we would get in the 90's.

Mr. TURNER. You know, we have had a large number of Members of Congress raise this question about why US-VISIT is based on a two-fingerprint system, rather than a 10. Some have suggested that even going to four would be a substantial improvement.

Do you understand and could you shed any light on why it is that the Department chose to stay with its two-fingerprint system, which apparently is much less effective in accomplishing our objective?

Mr. WEIN. To be honest, the last few years I have focused on other catastrophic terrorist events, namely, smallpox, anthrax, botulinum toxin and port security. So I have only been working on this problem for the last few months. I was not engaged in this problem at the time these decisions were going on. So I would guess other people in this room would have better answers to that.

I would—I think I will stop there.

Mr. TURNER. All right. My time may be up.

Mr. CAMP. Thank you.

Mr. Dicks may inquire.

Mr. DICKS. Thank you very much.

We have pointed this out to them, going all the way back to the time when they were selecting contractors. And I don't know why this—for some reason, they went for two, because it was easier and faster, I think.

This is something we pointed out to them; and I think they misled the committee, Mr. Chairman. I think the witnesses that were here misled our committee by not pointing out this problem with the unrecognizable or poorly done fingerprints.

I agree with you, I think terrorists are going to pick that up and understand that. So, I think we have to go to a 10-fingerprint system.

I have checked with some of the best experts in the world on this, and they all agree. In fact, NIST recommends a 10-slap fingerprint image stored in type 14.

You know, I think Congress—I think we have put in the reports recommending to them that they do this, that they compete it and have a competitive system. They didn't do it. I think it has something to do with the contractor, frankly.

But having said that, we have only got 3 minutes and 40 seconds. Tell us a little bit about these other issues. We know about this one. We know this is a mistake.

Tell us—you mentioned port security. Give us a couple of seconds on that.

Mr. WEIN. I have worked on the port security problem with Steve Flynn. I think, A, that is a much more important problem in the sense—it is one thing to let a terrorist into the country; it is another to let highly enriched uranium or a nuclear weapon into the country.

B, to their credit, I think it is a lot more difficult problem, the technology isn't all there.

C, I think they have been dropping the ball on this problem, and Steve Flynn and I have briefed Commissioner Bonner's entire staff. They have put all of their eggs in the ATS basket, and we are currently testing 5 percent of the containers; the other ones can waltz through the system.

It is easy for a terrorist to bypass one layer of security, particularly given the manifest rules that are in place. And we really need to do-100 percent passive radiation testing, and we need to do a fair amount of active testing in the sense of an x-ray or gamma ray imaging to look for shielding.

And we also need to spend money now to to find a way to detect highly enriched uranium, which is very difficult to catch with existing equipment.

Mr. DICKS. You mentioned a few others, anthrax and some other ones.

Mr. WEIN. For anthrax, I have an op-ed in the Washington Post, a paper in the Proceedings of the National Academy of Sciences. As a result of that, your area here, Washington, D.C., if a big attack occurs, the postal workers will help distribute antibiotics throughout the area. Hopefully, this program will go nationwide.

That was a direct result of our op-ed. I am currently funded by HHS to help them decide how, if and when to deploy the next-generation anthrax vaccine. My work on smallpox was instrumental in affecting the Bush administration's post-attack strategy for vaccination.

Mr. DICKS. We still don't have enough people vaccinated, though, do we? The caregivers, isn't that still a problem?

Mr. WEIN. Yes. The implementation of the front-line worker vaccination had a number of problems with it. And, you know—

Mr. DICKS. They still haven't been corrected, have they? They still don't have enough people vaccinated, do they?

Mr. WEIN. I think this—I think it is dead in the water at this point, until we have another terrorist attack, to be honest.

Mr. DICKS. In other words, to get more people vaccinated, the caregivers, we are going have to have a catastrophic event in order to convince everybody to do that? Is that what you are saying?

Mr. WEIN. It may not have to be catastrophic, but I think we need another event.

Mr. DICKS. Because nobody is paying attention? Is that what you are saying?

Mr. WEIN. No, it is not because no one is paying attention. It is because—it is several reasons. It is the risk communication, about what is the risk of—if I give the vaccine to the frontline worker, what are the chances of them dying or having a serious incident?

It is the perception of, is there really smallpox out there—the whole weapons of mass destruction in Iraq, issue. And it is a complicated problem.

Mr. DICKS. Well, again, I am troubled by this, Mr. Chairman, that we have had a series of these hearings. I commend the majority for having these hearings, but I think it is pointed out again and again and again, the deficiencies in this homeland security program.

And I don't know how we can, in the Congress, get people's attention in the executive branch that we have got to do more on these issues from port security, anthrax, the fingerprints for the US-VISIT program. I mean, there are all of these problem areas that haven't been addressed.

It is one of the things that has shocked me, frankly, in my service here in this Congress for 28 years. I have never seen something of this importance treated this way by the executive branch.

I commend the committee for having the hearings, because at least we have a chance to present the information to the American people. But we can't seem to get anybody to do anything about it.

Mr. Wein, I appreciate your going around and meeting with all of the officials. I hope that they will respond to your very lucid presentation of this gap in the fingerprinting program. I commend you for your good efforts, and please keep them up.

Mr. CAMP. Thank you.

That concludes our questioning. There being no further business, again I want to thank the subcommittee members and our witnesses for being here today.

The Chair notes that some members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 10 days—

Mr. TURNER. Mr. Chairman.

Mr. CAMP. —for Members to submit written questions to these witnesses and to place their responses in the record.

[The information follows:]

FOR THE RECORD

PLEASE NOTE: ASSISTANT SECRETARIES VERDERY AND HUGHES HAVE DEPARTED DHS. DEPUTY ASSISTANT SECRETARY FOR POLICY AND PLANNING ELAINE DEZENSKI SUBMITS ON BEHALF OF A/S VERDERY, MATTHEW BRODERICK, OF THE HOMELAND SECURITY OPERATIONS CENTER, SUBMITS ON BEHALF OF A/S HUGHES.

QUESTIONS FOR THE RECORD FROM CHAIRMAN CHRISTOPHER COX

1. Although the interagency charter for the Human Smuggling and Trafficking Center between the Departments of Homeland Security, State and Justice was just signed this past July, the 9/11 Commission's report itself referred to this center as having produced, "disproportionately useful results." The Commission staff believes that the collective interagency effort of the Center holds great promise to become one of the most important resources to combat terrorism and terrorist travel.

Q02133: Please describe for the Committee how the Department is currently working with the Human Smuggling and Trafficking Center and more importantly, what formal plans does the Department have and what steps has it taken to ensure that DHS does its part in ensuring this center reaches its full potential?

Answer: The Department of Homeland Security (DHS) supports the Human Smuggling and Trafficking Center (HSTC) in a variety of ways to enhance border security efforts:

- DHS has signed an interconnectivity agreement that provides HSTC personnel with access to critical DHS data systems to facilitate efficient information sharing;
- DHS procured necessary equipment to provide the HSTC with secure communications capabilities and provides the necessary systems support;
- Immigration and Customs Enforcement has assigned full-time staff to the HSTC that serve as subject matter experts in the areas of human trafficking, terrorist mobility and human smuggling. DHS is also committed to providing full time participation in the HSTC from other DHS components such as the United States Coast Guard (USCG), Customs and Border Protection (CBP), and Information Analysis.
- DHS utilizes the HSTC to convene important interagency coordination meetings, and to coordinate select initiatives. DHS also utilizes the products produced by the HSTC to inform the policymaking decision process.

DHS' commitment to the HSTC is long-term. DHS holds three seats on the HSTC Steering Group; Acting Under Secretary Randy Beardsworth is the DHS co-chair representative for the Steering Group, Elaine Dezenski, Acting Assistant Secretary BTS Policy and Planning, and Michael Garcia, Assistant Secretary of Immigration and Customs Enforcement, serve as members on the Steering Group for the HSTC. This group oversees and provides policy and administrative oversight of the HSTC, and to make sure that it is operating in a manner consistent with Constitutional liberties and national security requirements. Through this interagency Steering Group, DHS works with our partner agencies to ensure that the HSTC is fully supported by DHS, including personnel, fiscal resources, and information.

(B) Q02134: What specific budget authority and personnel resources does DHS plan to provide the HSTC?

Answer: In effecting the HSTC, DHS is more fully utilizing existing governmental facilities that have been associated with monitoring the flow of illegal persons, cargo and conveyances into the country. DHS is currently reviewing the re-

source requirements for the HSTC and anticipates that it will finalize both the operations funding and personnel requirements in the very near future. Currently there are 6 ICE agents/analysts staffing the Center full time and the USCG has 3 individuals on a part-time basis.

Additionally, the Director of the HSTC is a Department of Homeland Security (DHS) Immigrations and Customs Enforcement (ICE) Supervisory Special Agent.

(C) Q02135: How is the DHS Office of Information Analysis sharing information with the HSTC? And how is DHS as a whole going to share information with the Center?

Answer: Department of Homeland Security (DHS) Office of Information Analysis (IA) analysts have daily or near daily interaction with the management and staff members of the HSTC during which they discuss cables of mutual interest and collaborate on tasking and production. Cable traffic flagged by IA personnel is sent to the HSTC via SIPRNET (Secret Internet Protocol Router Network; the DoD-operated SECRET level network), as are all products classified SECRET and below that contain references to alien smuggling and terrorist mobility. If there are documents at a higher classification, IA will share hard copies with properly cleared HSTC members, and/or encourage HSTC to obtain the documents by other means. Once the HSTC is equipped with JWICS (Joint Worldwide Intelligence Communications System; the DoD-run TOP SECRET/Sensitive Compartmented Information system), all appropriate documents will be shared electronically. Information identified by HSTC staff is shared with IA in a similar fashion. Similar procedures are followed for information sharing between the HSTC and other enforcement and intelligence entities within DHS. HSTC personnel are able to access message traffic and finished production via connectivity to their parent organization systems and other online data repositories.

2. My staff had several meetings with the 9/11 Commission staff responsible for writing the terrorist travel portion of its report. And although not specifically articulated in the 9/11 Commission Report, its staff has pointed out in discussions with this Committee's staff combating terrorist travel will require "specialists" who are located at all ports-of-entry and that these specialists must have the ability to contact the intelligence community directly to obtain up-to-the minute classified information that could be used to combat terrorist travel.

Q02136: Please comment on this recommendation of Commission staff and indicate what concerns and roadblocks you see which might prevent this from occurring.

Answer: CBP worked diligently after release of the 9/11 Report to examine their findings and recommendations and make use of the report within CBP. Some of those recommendations will be incorporated into CBP practices and enforcement posture. By example, CBP is devoting extensive resources to training to make frontline officers more cognizant of the threat posed by terrorists and their weapons. To further this field level training, CBP's Office of Intelligence has placed an intelligence analyst at the Terrorist Mobility Group at the Terrorist Threat Integration Center (TTIC) to be aware of the trends and techniques and assist CBP with knowledge of these trends and methods to identify and defeat them. [1] We are participating in Joint Terrorism Task Force (JTTF) squads. We are nearly completing installation of a Special Compartmented Information Facility (SCIF) at the CBP National Targeting Center, with access to classified materials, to be able to support field enforcement—first and foremost, identification of terrorists and their weapons. Moreover, we work each day to apply whatever intelligence is derived from the Intelligence community into appropriate actions by field officers, in a manner consistent with the classification and sensitivity of the information. Our concerns would be more pedestrian—the length of time to obtain clearances for employees, which are needed to help work through the ever-growing volume of intelligence and classified material and the need for training employees to think and work as intelligence analysts do.

When CBP officer encounters a possible terrorist, they are required to contact the CBP National Targeting Center (NTC) and relay all the specifics of the individual for further review. In all cases where the NTC cannot discount the individual is a match to the terrorist, the Terrorist Screening Center (TSC) is contacted. The TSC has complete and full access to all of the derogatory information associated to the record and passes it back to the NTC when appropriate. The passing of information is only limited to the clearance level of the NTC officer and the security level of the communications into the NTC. The NTC, in turn, will relay enough information back to the port of entry (POE) for the front line officer to make appropriate decisions. The TSC will also contact the FBI Counter Terrorism Watch (CTW) with in-

[1] On December 6, 2004, the NCTC undertook all responsibilities assigned to the TTIC.

formation on the encounter. The CTW acts as the operational arm for the TSC and will relay operational instructions to CBP. They can also dispatch the local Joint Terrorism Task Force (JTTF) and have the ability to pass classified information to the cleared JTTF members.

There are two limitations to getting classified information to the POE. The first issue is the clearance level of CBP personnel in the field is rarely above the SECRET level and most derogatory information today is at the Top Secret and Code Word levels. The other issue is the lack of a secure communications path to the ports and how to get classified information to a non-SCIF environment. Two possible solutions are to make the NTC SCIF operational and/or to rely on the clearance levels of the JTTF teams. The JTTF approach is already in place and appears to be working.

3. As you are already aware, ICE's Forensic Document Lab is the only Federal crime lab dedicated almost entirely to the forensic examination of documents and has been doing so since 1978-and specializes in the identification of fraudulent visas and passports. Besides the FDL's role as the leading resource on fraudulent passports and visas to other Federal agencies, including the FBI and Department of State, the FDL's Library houses the largest known repository of known genuine travel documents. I have two questions related to the FDL,

(A) Q02137: Since the FDL is the leader in such documents, what concerns do you have that both the Department of State and the Department of Justice, both consumers of the expertise and resources available through the efforts of the FDL, may be planning to set up their own capabilities in the identification of fraudulent documents?

Answer: At present, we are not aware of any initiatives by either the Department of State (DOS) or Justice to develop their own capabilities in the identification of fraudulent documents. Several years ago, however, the DOS expressed an interest in establishing such a capability. When the Forensic Document Lab (FDL) learned of this, FDL representatives initiated a meeting with DOS officials to express their concern over the potential duplication of effort and unnecessary expenditure of resources. The FDL reiterated its willingness to provide forensic and operational support to all DOS entities. Subsequently, the DOS decided that its plan represented duplication of effort, and rather to continue to utilize the FDL's unique resources and expertise.

Central to the FDL's forensic and field operations support functions is its exemplar library, which presently contains more than 120,000 known genuine travel and identity documents and other resource materials from every country of the world. The library, the largest known collection of its kind and continually growing, represents a 25-year effort by FDL staff which would take enormous time and resources for another agency to replicate. A far more feasible and cost effective approach would be to dedicate additional resources to expand the FDL library and extend its availability to more federal, state, and local user agencies.

Q02138: And do you think that instead of duplicating efforts in other Federal agencies that instead more resources should be dedicated to the FDL and it expanded in light of the new importance being placed upon the disrupting of terrorist travel?

Answer: DHS agrees with the view of the 9/11 Commission Report that "targeting travel is at least as powerful a weapon against terrorists as targeting their money." DHS has devoted additional attention and resources to the analysis and disruption of terrorist travel. CBP has created the Fraudulent Document Analytical Unit (FDAU) to analyze the travel of suspected terrorists and the documents they use. CBP coordinates closely with ICE and the FDL so that the unparalleled experts at the FDL can forensically examine suspect documents, issue any necessary alerts, and modify the training in fraudulent document recognition that FDL offers accordingly. DHS believes that the FDL is the leading government entity in the identification of fraudulent travel documents and it would not be a prudent use of resources for other government agencies to seek to replicate the expertise that FDL already provides so well.

(B) Even with the FDLs limited resources and current staff of only 51, it impressively provides training to not only the agencies within DHS, (ICE, CBP, CIS, and the USCG), but also to other Federal agencies (State, Justice, IRS, SS Administration) and to state and local law enforcement and they can barely keep up with the requests for training currently.

Q02139: Please describe for the Committee how the Department plans to build upon the expertise of this office and enhance its ability to provide necessary training-including ongoing training-to DHS and other Federal agency personnel?

Answer: ICE is working to develop a strategy to establish an operational entity within the FDL to provide proactive, high quality training in fraudulent document recognition, specifically tailored to the needs of students from a wide variety of domestic and foreign law enforcement organizations, intelligence agencies, and private sector employers. In addition, the FDL would provide training courses and material to formally certify Document Instructors for DHS and other federal, state, and local agency personnel. The FDL would also develop training modules and presentations for use by ICE offices overseas in implementing outreach programs to educate and liaison with foreign enforcement agencies. The outreach materials would focus on document fraud and threat awareness training, and acquaint foreign officials with FDL capabilities and access protocols.

QUESTIONS FROM CHAIRMAN DAVE CAMP AND CHAIRMAN JIM GIBBONS

1. **Q02140 How is classified information disseminated to front line border and consular officials?**

Answer: In the U.S. Customs and Border Protection, classified information is reviewed by a team of intelligence analysts for information pertaining to terrorists attempting to enter the country or smuggle weapons of mass destruction into the United States. When appropriate, the analysts request a downgrade of information from the originating agency to put into the Sensitive but Unclassified (SBU) system that is available to the front line officers. This information could be as simple as the name of a person or as complex as performing analysis of various pieces of information to put into an intelligence alert or report, a trend analysis, or a threat assessment which again is entered into the SBU system.

Currently if classified information needs to be sent to the field, it is secure faxed or, if possible, verbally conveyed by way of STU/STE. CBP completed installation of the Homeland Secure Data Network (HSDN) in 24 offices in Calendar Year (CY) 04 for secure communications up to the Secret level.

The National Targeting Center (NTC) and Terrorist Screening Center (TSC) work together to identify and vet potential terrorists intending to travel to, or ship cargo to the U.S. and prevent them from entering or endangering the U.S. The NTC is a resource to CBP field officers for coordination and communication. It is also one of the TSC's largest customers for requesting additional identification of internationally traveling personnel or cargo that may have terrorist ties.

The NTC has the unique mission to provide a centralized communication point for all CBP field officers and a coordination center for all CBP Office of Field Operations anti-terrorism activities. This presents other agencies with the benefit of having a single point of contact (the NTC) for communicating anti-terrorism information and it ensures a coordinated, managed approach toward focusing CBP resources that is accountable across all levels of CBP.

2. The National Targeting Center (NTC), located in U.S. Customs and Border Protection (CBP), and the Terrorist Screening Center (TSC) both screen people and cargo using multiple databases.

Q02141: How do these centers work together and how do they distinguish their unique missions?

Answer: The NTC and TSC work together to identify and vet potential terrorists intending to travel to, or ship cargo to the U.S. and prevent them from entering or endangering the U.S. The NTC is a resource to CBP field officers for coordination and communication. It is also one of the TSC's largest customers for requesting additional identification of internationally traveling personnel or cargo that may have terrorist ties.

The NTC has the unique mission to provide a centralized communication point for all CBP field officers and a coordination center for all CBP Office of Field Operations anti-terrorism activities. This presents other agencies with the benefit of having a single point of contact (the NTC) for communicating anti-terrorism information and it ensures a coordinated, managed approach toward focusing CBP resources that is accountable across all levels of CBP.

It also has the added benefit of having entities knowledgeable about CBP operations conveying specific information regarding anti-terrorism efforts that is specific and germane to the operating environment.

The TSC is the clearinghouse for all encounters with known or suspected terrorists and as such is a significant resource for the National Targeting Center. Additionally, the NTC is the research center for CBP field officers for all potential terrorist or terrorism identifications. The NTC researches all terrorist field alerts and will contact the TSC for any additional classified derogatory information that may not be readily available to CBP field officers. By centralizing this capacity, clean,

secure lines of communication and roles can be established between the TSC and NTC. Through this process the TSC can contact the FBI Counter Terrorism Watch (CTW). The CTW, in turn, can dispatch the local Joint Terrorism Task Force (JTTF) and ensure an FBI case exists on the individual. In cases where an FBI case does not already exist, the National Joint Terrorism Task Force is contacted and they initiate a threat assessment on the subject. All information collected from the encounter is pushed back to DHS, FBI, NCTC and member of Intelligence Community (IC) for further analysis. The CTW coordinates the appropriate response through the NTC and they serve as the conduit for getting the appropriate information directly to the CBP field officers.

a. Q02142: Do these centers work with the Human Smuggling and Trafficking Center (HSTC)?

Answer: DHS can not speak for the TSC; however, the National Targeting Center is CBP's centralized anti-terrorism communication and coordination center for CBP's Office of Field Operations. As such, they routinely exchange available information with other agencies and their operations centers.

b. Q02143: How does the Department of Homeland Security envision these centers roles and responsibilities changing once the National Counterterrorism Center (NCTC) is created?

Answer: CBP sees the role of the NTC becoming even more significant once the NCTC is created. There will continue to be a need for CBP to centralize its anti-terrorism communication and coordination with its field assets. The need for the NTC will continue to be vital for managing effective and efficient communications from external sources and passing it down to CBP field officers, as well as, collecting information internally from CBP field officers and passing it up to external sources. A side benefit from this accountability process is that the NCTC or other centers are not responsible for knowing how to best communicate information to CBP field officers in and between over 300 ports, or have telephone lists.

3. Homeland Security requires a strong international security policy. The Department of State is the face of the U.S. Government overseas and is our first line of defense, through the visa review process, against potential terrorists entering the United States.

Q02144: How does DHS share information with State Department?

Answer: State's Consular Lookout and Support System (CLASS) receives over 3 million watch-listings from DHS systems, including the Treasury Enforcement Communications System (TECS).

In the context of visa security specifically, State Department shares visa applicant and adjudication data with the Visa Security Program, and the Visa Security Program shares the results of its reviews with State. State also provides watch-listings and lost and stolen passport information to TECS (over 850,000 records).

USCIS' Office of Fraud Detection and National Security (FDNS) meets on a monthly basis with DOS' Office of Fraud Prevention Programs to discuss cross cutting issues. In addition, FDNS is drafting a Memorandum of Understanding (MOU) with DOS's Visa Office (VO) on data sharing. Pursuant to the MOU, USCIS will obtain access to DOS' Consolidated Consular Database (CCD) and certain reports and systems accessible through the CCD and DOS will be granted access to certain USCIS databases.

During the visa application process, biometric and biographic information collected by consular offices is queried against selected databases via an electronic interface with US-VISIT. At the POE, the inspecting office can verify biometric and biographic information provided by the travel against the DOS visa information through US-VISIT.

Q02145: Are there common training programs regarding terrorist indicators and fraudulent documents?

Answer: In the context of visa security specifically, the Visa Security Program is developing a training program for consular officers that will address numerous issues relevant to effective consular adjudication of visa applications, including terrorist indicators and fraudulent documents. These trainings will leverage training material that is included in the Program's training curriculum for Visa Security Officers. The FDL does provide fraudulent document training to State and other agencies and will continue to do so.

4. Is the following available to DHS personnel including front line agents? If it is, what agency provides this information?

(A) Q02146: The number and type of fraudulent documents used broken down by country over the past month, quarter, or year?

Answer: CBP collects information on fraudulent documents in several ways. One source is through its statistical collection Form G–22 Inspections Workload Report

provided by the ports of entry. The Form G–22 data provides only the number of various types of fraudulent documents intercepted, but does not provide the country of origin. In January 2005, CBP established the Fraudulent Document Analysis Unit (FDAU), now the collection point for fraudulent documents confiscated at the ports. The FDAU collects additional categories of statistics, to include the number of passports, country of origin, and the nationality of the person who presented the document, and conducts regular analysis of fraud trends and significant interceptions which will be disseminated to DHS front line agents. The FDAU expects to have data ready in these categories by July for the first six months of this calendar year. The United States also intercepts other fraudulent travel documents in addition to passports, including Mexican border crossing cards and U.S. permanent resident cards. The FDAU expects to disseminate statistical information on fraudulent travel documents to the ports and others every six months.

(B) Q02147: Information regarding stolen and fraudulent passports and documents acquired from collection activities abroad?

Answer: It is crucial that component frontline CBP officials receive information regarding lost, stolen and fraudulent passports (or other travel documents). CBP systematically receives reporting from the Department of State and other federal agencies regarding lost and stolen passports and fraudulent documents. This information migrates to CBP Inspectors via electronic interface through the Treasury Enforcement Communications System (TECS) and the Consular Lookout and Support System (CLASS). Additionally, the DHS Office of Information Analysis (IA) and other Intelligence Community (IC) members periodically produce and disseminate lengthier pieces of unclassified finished intelligence for line agents. Such products may address trends, such those pertaining to lost and stolen passports, or may be crafted as specific hands-on guides. There are ongoing initiatives to improve the speed at which classified data is made available to line agents at the UNCLASSIFIED level. For example, IA is working with the IC to establish a standard whereby the pertinent portions of classified information concerning lost and stolen passport information will be automatically downgraded so that the information can immediately be sent to CBP's National Targeting Center. This would allow the frontline officers to more quickly query the Interagency Border Inspection System (IBIS) database to ascertain if the passport is from a lost/stolen batch or known fraudulent document. The FDL's Operational staff provides seven day a week (and Holidays) assistance to CBP field personnel regarding fraudulent documents. The Operations staff has access to the largest collection of foreign and domestic travel and identity documents in the world. They also have access to the Image Storage and Retrieval System (ISRS—photos, fingerprints and signatures from tens of millions of "green cards" and Employment Authorization cards), DOS's DataShare (database of photos and biographical data from millions of U.S. non-immigrant visas and U.S. passports), EDISON (image database of passports of every country in the world and other DHS databases. The FDL officers themselves have many years experience in examining travel and identity documents. The operations staff develops and disseminates Document Intelligence Alerts, Document Reference Guides and Fraudulent Document Briefs. They also develop and conduct fraudulent document training for CBP officers. As part of the Department's work in this area, the DHS Privacy Office is working collaboratively with other program offices to research the pragmatic, policy and privacy protection issues related to a distributed model for the exchange of passport-related data (lost, stolen, identity verification) where participating governments would control access to the personal information of their travelers and be able to verify travelers and travel documents of others in real time.

(C) Q02148: On site resources at high traffic ports of entries to assist agents in identifying fraudulent documents or terrorist indicators on documents?

Answer: Most high traffic ports of entry have the EDISON system on site. This is a computerized database containing images of travel documents and their security features from all countries. The system is used for comparative purposes when examining questioned documents. Altered and counterfeit documents are also contained in the database for reference.

Ports have on site training staff and reference documents to assist Officers in identifying fraudulent documents or terrorist indicators. Immigration and Customs Enforcement (ICE) Forensic Document Laboratory (FDL) provides all ports with immediate assistance in document verification through their Intelligence Officers. The FDL produces and distributes Document Alerts to the ports illustrating recent fraudulent document interceptions.

The Customs and Border Protection (CBP) Fraudulent Document Analysis Unit (FDAU), as it comes on line, will provide both strategic and tactical information to

ports of entry regarding recent trends of document abuse identified through an analysis of document interceptions at ports of entry. This information will enable CBP officers to be on the alert for new patterns of fraud.

5. Q02149: What is the Department doing to deal with the problem of altered and counterfeit passports and visas?

Answer: The FDL's Operational staff provides seven day a week (and Holidays) assistance to all DHS personnel, other federal agencies, foreign immigration/border control authorities, State and local police and DMV and Social Security personnel in all matters relating to fraudulent documents. The Operations staff has access to the largest collection of foreign and domestic travel and identity documents in the world. They also have access to the Image Storage and Retrieval System (ISRS—photos, fingerprints and signatures from tens of millions of "green cards" and Employment Authorization cards), DOS's DataShare (database of photos and biographical data from millions of U.S. non-immigrant visas and U.S. passports), EDISON (image database of passports of every country in the world and other DHS databases. The FDL officers themselves have many years experience in examining travel and identity documents. The operations staff develops and disseminates Document Intelligence Alerts, Document Reference Guides and Fraudulent Document Briefs. They also develop and conduct fraudulent document training for all DHS personnel, other federal agencies, foreign immigration/border control authorities, State and local police and DMV and Social Security personnel **(FDL's longstanding relationships)** The FDL has continually participated in international working groups and conferences for over 20 years. The FDL was instrumental in the creation of the International Immigration Fraud Conference (IFC) which is comprised of 20 Western European and North American countries) that meet annually to exchange information on document fraud, fraudulent document training and document examination equipment. The FDL has also participated in Interpol's Fraudulent Document Working Group that develop minimum standards for passports. The FDL chaired the Security Working Group to develop minimum standards for U.S. driver's licenses and identification cards mandated by the Intelligence Reform Act of 2004.

We are working well with our international and interagency partners on improving standards for travel documents, aviation safety, port security and the exchange of watchlist information. The appropriate and secure use of biometric identifiers will assist in all these efforts. We use biometric identifiers as tools to help prevent the use of fraudulent travel documents and identities so that we can be more confident and secure about our admissions and screening decisions. DHS has conducted a review of the use of biometrics to ensure that we are coordinating the implementation of biometric technology across the Department. In the international arena, we are working closely with our European counterparts in the G–8, the International Civil Aviation Organization (ICAO) and other international fora to discuss how to advance biometric methodologies, both in chip technology and electronic readers, by establishing standards to ensure global interoperability.

The most notable success in our efforts is the creation of US-VISIT, a biometric entry-exit system. This system not only allows the Department to know who has entered the United States, but also captures a photograph and scans of index fingers to prevent the use of fraudulent identities to circumvent detection and employs biometric visa data shared by the US Department of State. In addition, the US-VISIT data is shared with law enforcement and intelligence agencies as appropriate. Other initiatives undertaken by the Department include the promulgation of regulations to ensure that passenger data is collected and provided to law enforcement agencies for screening purposes, including efforts to target terrorists through the National Targeting Center; participation in the G8 Lyon Roma group focusing on terrorism; setting passport issuance standards and fraud prevention.

Q02150: How is the Department working with other federal agencies to deal with this problem?

Answer: The Department utilizes the resources of the Forensic Document Laboratory to ensure that information about fraudulent documents is disseminated to appropriate agencies within and outside the Department. Distribution of "Document Alerts" based on information obtained from intercepted fraudulent documents will be the major ports of entry throughout the United States, ICE, CBP, and CIS offices, Federal law enforcement training centers, various law enforcement intelligence services, the US Department of State, the US Secret Service, and the US Federal Protective Service. When appropriate, alerts will also be sent to the Social Security Administration, relevant Department of Motor Vehicles, and several transportation trade organizations such as the International Civil Aviation Organization, National Maritime Organization and International Council of Cruise Lines. The

widest distribution of information on altered/fraudulent travel document is essential to addressing the problem.

6. Q02151: Describe in detail the technologies and training methods the Department is using to detect terrorist indicators on travel documents.

Answer: In the context of visa security specifically, the Visa Security Program is training its officers in terrorist indicators and document evaluation. The Program is leveraging the resources of ICE Forensic Document Laboratory (FDL). CBP and the FDL have created a train the trainer session that has brought in more than 300 CBP Officers into the FDL for a 3-day intensive training session. They stay another day and are given the material they will take back to the port in order to teach an 8-hour course. This course is currently a prerequisite to some of our cross training efforts, such as our Anti-Terrorism Passenger course and Unified Primary. As of November 5, 2004, more than 4566 Officers have participated in this 8-hour course. In addition, using advance passenger information, the National Targeting Center accesses a variety of databases to identify travel and document patterns which might indicate terrorist connections.

Q02152: Again, how is the Department coordinating its efforts with other federal agencies?

Answer: In the context of visa security specifically, the Visa Security Program coordinates closely with State. At posts where Visa Security Officers are deployed, the VSOs work closely with consular officers; share information about fraud documents, fraud schemes, and terrorist activity and indicators; and provide training to enhance consular officers? ability to recognize those during the consular adjudication process. The VSOs also work with the law enforcement and intelligence communities at post and share information to support their efforts.

The HSTC is utilized by DHS to convene important interagency coordination meetings, and to coordinate select initiatives and has signed an interconnectivity agreement with the HSTC that allows HSTC personnel, including non-DHS personnel, to access DHS information systems. DHS has also provided information technology resources to provide secure communications capabilities to HSTC personnel. Equally important, however, numerous agencies are able to communicate directly with the HSTC's staff on a daily basis on a wide range of policy, intelligence, and operational issues that impact our efforts to secure the homeland.

7. Q02153: Is the training provided to our front line border personnel sufficient?

Answer: Together with the FDL, we have created a train the trainer session that has brought in more than 300 CBP Officers into the FDL for a 3-day intensive training session. They stay another day and are given the material they will take back to the port in order to teach an 8-hour course. This course is currently a prerequisite to some of our cross training efforts, such as our Anti-Terrorism Passenger course and Unified Primary. As of November 5, 2004, more than 4566 Officers have participated in this 8-hour course.

Q02154: Or do we need a terrorist travel specialist at our ports-of-entry who can provide this information but also protect classified information?

Answer: The trainers described above, however, are not only equipped to teach this single course, but now have the materials and technical experience to teach additional port specific material. These are the technical experts and this pool of personnel will continue to expand, with the continued help of the FDL.

As noted, CBP will establish a complementary function at selected field locations to ensure that there will be a specialist available to ports of entry at all times. This unit, and the field specialist, will work closely with the CBP Office of Intelligence and the intelligence community as a whole to ensure our front line border officers have the best and most up-to-date information available to safeguard the United States.

Q02155: Do all the front-line personnel who need clearances to utilize current threat information in their activities have the appropriate clearances?

Answer: All appropriate front-line personnel who need clearances have them or are in the process of obtaining the required clearances.

8. Q02156: What is the Department doing to uncover clandestine travel among terrorists?

Answer: The Department has instituted a number of initiatives designed to target clandestine travel by terrorists. As noted in the 9/11 Commission Report, targeting terrorist travel is a powerful weapon, and constraining terrorist travel is part of the Department's overall strategy. As part of this effort, we are working well with our international and interagency partners on improving standards for travel docu-

ments, aviation safety, port security and the exchange of watchlist information. The appropriate and secure use of biometric identifiers will assist in all these efforts. We use biometric identifiers as tools to help prevent the use of fraudulent travel documents and identities so that we can be more confident and secure about our admissions and screening decisions. DHS has conducted a review of the use of biometrics to ensure that we are coordinating the implementation of biometric technology across the Department. In the international arena, we are working closely with our European counterparts in the G–8, the International Civil Aviation Organization (ICAO) and other international fora to discuss how to advance biometric methodologies, both in chip technology and electronic readers, by establishing standards to ensure global interoperability.

The 9/11 Commission Report also advised that the Department needed to look even more closely at our aviation security initiatives and give special attention to improving each of the layers of the security system. The improvements in the layered approach include using biometric identifiers as well as using airline passenger data appropriately—both passenger name record (PNR) data and advanced passenger information system (APIS) data, which are screened against law enforcement databases by the National Targeting Center.

The most notable success in our efforts is the creation of US-VISIT, a biometric entry-exit system. This system not only allows the Department to know who has entered the United States, but also captures a photograph and scans of index fingers to prevent the use of fraudulent identities to circumvent detection employs biometric visa data from US Department of State. In addition, the data is shared with law enforcement and intelligence agencies as appropriate. Other initiatives undertaken by the Department include the promulgation of regulations to ensure that passenger data is collected and provided to law enforcement agencies for screening purposes, including efforts to target terrorists through the National Targeting Center; participation in the G8 Lyon Roma group focusing on terrorism; setting passport issuance standards and fraud prevention; continuation of the National Security Entry Exit Registration System (NSEERS) for special interest travelers; and the use of the Student and Exchange Visitor Information System or SEVIS to monitor the activities of foreign students. Additionally, the Department is actively working with the FBI and the Department of Justice, which already provides terrorist and criminal fingerprint data to US-VISIT to allow FBI access to data collected by US-VISIT at the ports of entry. Through these and other efforts, and the sharing of data with the appropriate agencies, the Department is working diligently to uncover clandestine travel by terrorists.

DHS has coordinated improvements to security in the maritime arena by its implementation of a layered system of screening vessel arrivals to the U.S. Since 9/11, the USCG has been added as formal member of the Intelligence Community, created Maritime Intelligence Fusion Centers on the Atlantic and Pacific coasts, begun fielding Field Intelligence Support Teams in major U. S. ports, created the National Vessel Movement Center, and created the Coastwatch Program at the Intelligence Coordination Center in Suitland, MD. All of the programs are interagency coordinated efforts to bring together federal, state, and local agencies with a role on the protection of maritime assets an infrastructure. They all play significant roles in screening and collecting intelligence information on arriving ships, crew, and passengers that enter the U.S.

In addition, the services and unique expertise of HSTC personnel directly supports the Commission's call for enhanced connectivity amongst law enforcement and intelligence entities. This enhanced connectivity will improve the U.S. Government's effectiveness in combating terrorism, as well as supporting an enhanced worldwide focus on travel and identity document fraud. Furthermore, the HSTC's interagency environment provides the opportunity to apply this approach to the serious problems of human trafficking and human smuggling.

For the first time, the HSTC brings together federal agency representatives from the policy, law enforcement, intelligence, and diplomatic arenas to work together on a full-time basis to achieve increased progress in addressing the problems of human smuggling, human trafficking and clandestine terrorist mobility. Additionally, the HSTC has access to several interagency, national, and international databases that contain information relative to human smuggling and human trafficking that may not be readily available through other sources. This combination of on-site expertise and accessibility to sensitive information provides the U.S. Government and foreign allies with a unique opportunity to more effectively identify and dismantle smuggling and trafficking organizations, and terrorist travel facilitators by working together to attack these threats on multiple fronts.

9. Q02157: How is the Department developing techniques to counter the evasive methods terrorists use to travel?

Answer: The Department is actively involved in developing techniques to counter evasive methods used by terrorists to travel. Through the use of biometrics and the US-VISIT program, the use of fraudulent identities to enter the United States can be effectively countered. Through US-VISIT, and in conjunction with the Department of State's Biometric Visa Program, the Department has created a "virtual border" as a line of defense against entry by terrorists. Travelers seeking visas are screened against biometric and biographic watchlist to identify criminals, terrorists, and immigration violators. DHS is also working internationally to counter terrorist travel by participation in the G8 Lyon Roma group targeting terrorism and the use of fraudulent identification documents. In addition, the Department is in the process of implementing the legislative mandate of Section 428 of the Homeland Security Act. The Department will deploy experienced DHS law enforcement officers to U.S. embassies and consulates. These officers will perform in-depth investigative reviews of high risk visa applicants, conduct training programs for Department of State consular officers, initiate investigations, conduct homeland security law enforcement liaison, and research and disseminate intelligence.

The Department is also home to the Forensic Document Laboratory, the premiere fraudulent document laboratory in the world. It maintains an extensive library of travel documents, as well as trained forensic experts and intelligence officers who provide expertise throughout the Department.

For aviation travelers, the department collects advance passenger information system data (APIS) otherwise known as manifest data, which is screened against law enforcement data bases and watch-lists. For specific flights, the Department also collects and vets passenger name record (PNR) data which may contain more detailed information about the passenger's itinerary. In addition to using passenger date, DHS has also piloted the Immigration Advisory Program (IAP) through which small teams of CBP Immigration Advisory Officers with strong immigration backgrounds are assigned to foreign airports to work with host country officials to identify potentially high-risk or inadmissible passengers before they board planes bound for the United States.

DHS recognizes that there is no single solution to prevent airplanes from being used as weapons of terrorism. The improvements in the layered approach include using biometric identifiers to deter visa fraud, sharing lost and stolen passport information through Interpol, promoting a global standard for machine readable passports, using airline passenger data appropriately, expanding no-fly lists, screening domestic and international passengers against no-fly lists, including more travelers in US-VISIT, boosting airline security utilizing Federal Air Marshals on international flights of concern, hardening cockpit doors, and offering voluntary programs for arming pilots on passenger and cargo planes for domestic flights.

Through the collection and dissemination of information, through the use of biometrics, and new approaches and technology such as US-VISIT, the Department is constantly seeking out ways to detect and counter the evasive methods used by terrorists to travel.

In addition, the HSTC staff is collecting, correlating, analyzing and disseminating domestic and international information on clandestine terrorist travel on a continual basis. These activities include:

- Daily SECRET cables from select U.S. government sources via DOS Cable Xpress.
- Daily notices of activities, items of interest, and intelligence from domestic, overseas and foreign sources.
- National and foreign fraudulent document alerts.
- Consular fraud notices and intelligence alert bulletins.
- Foreign law enforcement reports, notices and alerts.
- Foreign government periodic reports on:
  - Immigration
  - Identity and travel document fraud
  - Terrorism
  - National Security

The HSTC will support and exchange information with the NCTC and other U.S. agencies and organizations active in the war on terrorism, trafficking in persons and human smuggling. It will also coordinate feedback amongst the various diplomatic, law enforcement, and intelligence agencies.

10. International coordination is essential to prevent terrorists from traveling into our country.

Q02158: What is the Department doing to coordinate with the international community to prevent terrorist travel?

Answer: The 9–11 Commission Report stated: **"The U.S. government cannot meet its own obligations to the American people to prevent the entry of ter-**

rorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation." The bombings in Madrid, the more recent hostage crisis in Beslan, Russia and the Australian Embassy bombing in Jakarta also serve as vivid reminders to us that terrorism is an international threat that cannot be conquered alone. DHS understands that we must engage in a global effort each day, through collaboration, information sharing and ongoing dialogue to ensure that our efforts are informed, coordinated, and effective.

As part of this effort, we are working well with our partners bilaterally and within multilateral organizations to improve standards for travel documents, aviation safety, port security and the exchange of watchlist information.

The Department is working closely with our the international partners in the EU as well as with Canada, Mexico and other foreign governments to ensure that developments and initiatives in border and transport security are discussed, coordinated, and clarified before they are implemented.

We are taking such steps every day. For example, together with our colleagues in the Department of State, DHS is addressing security challenges posed by lost and stolen passports. Through the efforts of the Departments of State and Justice, the U.S. has provided over 300,000 records of Lost and Stolen passports to the Interpol's lost and stolen document database, which is available to border authorities worldwide. We continue to encourage our international partners to join us in this effort. Additionally, the US is initiating a scoping study to assess a technology concept that helps address this concern. The Enhanced International Travel Security (EITS) concept, which has been addressed in the G–8 context, uses distributed databases as a mechanism to allow real-time exchange of to the basic information needed- i.e., a "yes" or "no" response—concerning the validity of a document without requiring visibility into the data that allows that determination. The approach would be very similar to that already used worldwide by the banking industry to support ATMs. Developing better systems for international sharing of information, and expanding participation to more countries will improve our ability to identify and screen travelers before they enter our country.

Another area on which we are working to make significant enhancements involves the Visa Waiver Program and US-VISIT. DHS, with the assistance of Department of State, is in the process of completing the country evaluations required under the Visa Waiver Program statute. These reviews involve site visits to each of the participant countries. Overall, the cooperation of the VWP countries' governments has been exceptional. Additionally, on September 30, 2004, we began processing nationals from VWP countries through in US-VISIT. The Department engaged in multiple forms of outreach to ensure the countries and their citizens were prepared for the expansion of the program.

To address possible risks, prior to flight departure, the Department has piloted the Immigration Advisory Program (IAP) in Poland and the Netherlands and is exploring other locations to expand this program. Host countries have shown support for this reciprocal program that has CBP officers assisting in examining travel documents and screening the flight manifests to make determination of whether passengers are adequately documented or likely to be found inadmissible upon arrival in the United States. Such efforts save the air carriers from penalties and providing an extra layer of security prior to departure.

Since the establishment of the Department, the leadership of DHS has worked to establish and enhance the critical international relationships and partnerships with foreign counterparts. Coordinated efforts and continuous dialogue have proven vital to pursuing the DHS mission, whether it be through well-established legacy agency dialogues with Mexican and Canadian neighbors, the new Joint Contact Group meetings with United Kingdom officials that examine issues relating to all aspects of Homeland Security, the continuous discussions with European Union (EU) and the EU Member States. In addition, Department officials engage with foreign partners within the various international fora such as ICAO, World Customs Organization (WCO), International Maritime Organization (IMO), the G–8, Organization for Security and Cooperation in Europe and many others.

DHS has also connected the Canadian Government Operations Center, the United Kingdom's Civil Contininginccies Secretariat, National Security Advice Center, to the Homeland Security Information Network. This network provides 24/7 connectivity, at the SBU level, from each of these locations to the Homeland Security Operations Center.

Q02159: How is the Department working with our neighbors, in Canada and Mexico in particular, to devise a coordinated anti-terrorist travel strategy?

ANSWER: The Department values the strong partnership of the Governments of Canada and Mexico in securing international travel. While the work plans with our neighbors are similar in many respects, they are also tailored to the specific capacities and realities of each government. We are proceeding on two bilateral tracks rather than a trilateral track at this time although there is strong potential for convergence the future.

On December 11, 2001, the U.S. and Canada signed a *Smart Border Plan* originally containing 30 concrete initiatives to secure the infrastructure, flow of people, and flow of goods and to share information. A few short months later in March 2002, the U.S. and Mexico signed a 22-point *Border Partnership Action Plan* organized under the pillars of secure movement of goods, secure movement of people, and secure infrastructure. Together with our neighbors we recognized that our current and future prosperity—and security—depend on borders that operate efficiently and effectively under any circumstance.

General

Progress is steady and many of the initiatives have already been implemented or are near completion. In other cases, on-going processes are required. Others, like our cooperation on human smuggling and trafficking, are ongoing activities that continue to be strengthened as we deepen our relationships. Some goals will require many years and extensive investment before they are in place. In some cases, such as the electronic sharing of information, the process is itself the goal. Still in other cases, long-term investment, political will and effort will be necessary to achieve the goal.

APIS

Of particular note is the progress in sharing advanced passenger information. Currently, Canada and Mexico require international air carriers to send electronically manifest information for commercial flights destined to their countries. We are vetting the APIS data against relevant databases and have already developed with Canada a means to exchange bulk and individual records. Additionally, Customs and Border Protection (CBP) has developed common risk-scoring algorithms with its Canadian colleagues as well as a mechanism to resolve hits. Under the U.S.—Mexico Smart Border Action Plan, the GOM transmits APIS data to CBP. Commercial air carriers transmit API data to the GOM as required by law. The Mexican API data is retransmitted by the GOM to CBP via the existing CBP APIS infrastructure. In May 2004, the GOM designated Centro de Investigación y Seguridad Nacional (CISEN) as the lead point of contact for the Mexican APIS program.

Integrated Border Enforcement Teams (IBET)

In support of the Canada-United States Smart Border Declaration and Action Plan for creating a secure and smart border, Integrated Border Enforcement Teams (IBETs) seek to identify mutual national security threats and combat illicit cross border activity. IBETs are multi-agency field level groups of law enforcement officials dedicated to securing the integrity of the Canada/United States border while respecting the laws and jurisdictions of each nation. The IBET mission is to enhance border integrity and security at our shared border by identifying, investigating and interdicting persons and organizations that pose a threat to national security or are engaged in other organized criminal activity.

Across the northern border, 15 regional IBET locations have been established and are currently active. Each IBET has a local Joint Management Team (JMT) to incorporate national policies and formulate local investigative priorities of the regional team. The JMT is predicated on the needs and involvement of its participating agencies.

IBETs are not "firehouses" waiting for something to occur but rather operate as intelligence driven enforcement teams comprised of federal, state/provincial and local law enforcement personnel to address terrorism and other forms of criminality in the context of the border. The teams are multidisciplinary in nature and work in an integrated land, air, and marine environment along or near the Canadian/United States border while respecting the jurisdiction of each nation.

The IBETs were developed to be "intelligence driven" units. The concept of the Joint Intelligence Teams is to develop an inter-connectivity of intelligence by co-locating ICE Intelligence Analysts/Intelligence Research Specialists and Special Agents with Intelligence Analysts/Officers representing the other participating core member agencies. The intelligence officers will be responsible for the collection and

collation of information and its dissemination to the field, other IBETs, as well as to their respective Headquarters entities.

Cargo Screening

Tremendous progress has been made in securing commercial traffic—both rail and truck. By 2005, it is expected that 100% of rail cargo entering the U.S. from Canada and Mexico will be screened using Vehicle and Cargo Inspection Systems (VACIS) and other appropriate technologies. The benefits derived from our northern and southern border FAST programs speak for themselves. For example, 92% of commercial traffic on the US-Mexico border is via the FAST lanes at the seven largest ports. We have aggressive expansion plans for FAST along the southern border and are studying additional dedicated FAST lanes at some of the busiest crossings between the U.S. and Canada.

The Department, through CBP, has developed with Canada a Joint Targeting Initiative to review and research bills of lading and manifests necessary to target high-risk containers destined for North America. Additionally, CBP and Canada will embark on a common Container Security Initiative, leveraging resources at select locations abroad.

Passenger Enrollment Systems

Low-risk, pre-enrolled travel programs for visitors and other non-commercial travelers are another example of ways to leverage technology and bilateral cooperation to achieve the mutual goals of enhanced security and facilitated through-flow of known border crossers. We continue to expand and upgrade the NEXUS and SENTRI programs at our land borders while ensuring continuous compliance monitoring. Further, we will test a NEXUS Air program with Canada at the Vancouver International Airport.

Visa Policy

Visa policy plays an essential role in our layered defense strategy that prevents known high-risk travelers from entering North America. To this end, we are working with Canada and Mexico to identify commonalities, gaps and areas. For example, since September 11, Canada has imposed a visa requirement on nationals of 12 countries, including Saudi Arabia and Malaysia. We are studying ways to converge visa-screening procedures and to exchange visa information.

Information Sharing

Both before and since the terrorist attacks of September 11, 2001, the State Department, with DHS and other interagency partners, has spearheaded efforts to coordinate the exchange of biographic terrorist screening information. With the specific authority granted to the Secretary of State by the USA PATRIOT Act of 2001 to establish agreements with foreign governments on exchange of visa screening information, we are seeking to negotiate more robust information exchange agreements.

On June 12, 2003, the Secretary of State authorized negotiations on an agreement for the systematic exchange of broader visa screening database information with Canada and approved a draft executive-level agreement to do so. At the same time, he gave blanket authorization to pursue such an agreement with any other willing country, using the effort with Canada as a model. In accordance with the new guidelines of the Homeland Security Act, the State Department sought the cooperation of DHS and subsequently the newly formed TSC. In January 2004, the State Department opened negotiations with Canada aimed at reaching such an agreement. The negotiating team, which includes representatives of State, DHS and the TSC, is addressing the policy, legal and technical issues involved.

The HSPD–6 Memorandum of Understanding (MOU) on the Integration and Use of Screening Information to Protect Against Terrorism of September 16, 2003 was signed by the Departments of State, Justice, and Homeland Security and the DCI. The MOU requires the obtaining of terrorist screening information from our foreign partners "in a manner consistent with each government's laws," and, as necessary, "to provide operational support to the participating governments." It also established the guidelines for operation of the TSC and the transfer of State's TIPOFF database to the TTIC. The TIPOFF Program, founded in 1987, was the first federal program focused on the identification of known and suspected terrorists to prevent their entry into the United States. On November 17, 2003 the TTIC,[2] under the authority of the DCI, assumed responsibility for TIPOFF and for collecting all information the U.S. Government possesses related to known or suspected terrorists, with the exception of information on purely domestic terrorists. TIPOFF contains more than 175,000 records on terrorist identities as of mid-August 2004 and serves as a

[2] On December 6, 2004, the NCTC undertook all responsibilities assigned to the TTIC.

screening and analytic resource to the U.S. Government. On December 1, 2003 the Terrorist Screening Center (TSC) was established, under the administration of the FBI, to consolidate the U.S. government's approach to screening for terrorism.

The TSC facilitates terrorist screening exchange arrangements with two trusted partners—Canada and Australia. An agreement with Canada was established and implemented on May 23, 1997, and with Australia on April 12, 2000, through which sensitive but unclassified biographic screening data elements derived from the Terrorist Screening Data Base (TSDB), were made available to both countries. Terrorist screening data provided to TIPOFF by Canada and Australia is included in the Consular Lookout and Support System (CLASS) used by the State Department to screen visa applicants in the Integrated Border Inspection System (IBIS) used by DHS to screen travelers seeking admission into the United States, and by other federal, state, and local law enforcement through the National Crime Information Center (NCIC). HSPD–6 also tasked the Department of State, in conjunction with the TSC, to expand the sharing of terrorist identifying information with other countries and to begin with our partners in the Visa Waiver Program. This effort has been initiated and significant progress is being accomplished.

Similarly, we are working within the Administration to determine the appropriate bilateral exchange of the No Fly and Selectee Lists currently used by domestic and international airlines transporting passengers in, to, or from the United States to conduct passenger prescreening. We continue to monitor the status of domestic legislation in Canada that would further enhance aviation security including the exchange of passenger information on domestic flights that may fly over U.S. airspace.

Transportation Security

Member States in the International Civil Aeronautics Organization must meet the 100% hold-baggage screening standard by January 2006. This standard will make the global aviation system even more secure and will help reduce the possibility of acts of terrorism on our air carriers. The Department is pleased that our neighboring governments are sharing information to help meet this goal.

US-VISIT

DHS implemented US VISIT at 115 airports and 14 seaports starting on January 5, 2004. The land border solution is being designed to be fast and easy, but also secure. The Department is committed to the dual goals of enhanced security and facilitated legitimate travel. Through US-VISIT, and in conjunction with the Department of State's Biometric Visa Program, the Department has created a "virtual border" as a line of defense against entry by terrorists. Travelers seeking visas have their fingerprints vetted against a biometric watchlist to identify criminals, terrorists, and immigration violators We have worked closely with officials from Canada and Mexico to develop an effective and open communication mechanism to exchange ideas and address concerns about how US-VISIT utilizes technology, how it may affect border communities, and how to manage public relations. Shared infrastructure, biometrics, data privacy and protection are all issues of common interest. The Department looks forward to continued bilateral dialogue as US-VISIT expands to the 50 largest land border ports by December 2004 and all land ports by December 31, 2005, and as we assess and build upon technologies and management concepts being tested or already deployed from the various departure pilots.

11. Constraining terrorist mobility should be a broad, long-term DHS goal.

Q02160: What initiatives does DHS have underway and what have you identified as future goals or developing capabilities?

Answer: CBP has a number of initiatives underway in support of DHS's long-term goal of constraining terrorist mobility. To highlight a few:

Deploying Immigration Advisory Officers

The Immigration Advisory Program (IAP) is a CBP effort to prevent terrorists from entering the United States. Under IAP, small teams of CBP Immigration Advisory Officers with strong immigration backgrounds would be assigned to the major "hub" airports around the world to identify potentially high-risk or inadmissible passengers before they board aircraft bound for the United States. Through these efforts, CBP is better positioned to address the worldwide threat of terrorism.

CBP initiated an IAP pilot at Amsterdam's Schiphol airport on June 26, 2004 and a second effort began at Warsaw's Chopin Airport on September 15, 2004. The IAP teams in both foreign locations have established similar passenger processing methods. Typically, airline security officers or government border guards review passenger documents and if there are any anomalies with the document or the passenger, they request assistance from the IAP Officer. IAP officers, based on targeting information or observation, may ask to see a particular passenger. Based on the review of the passenger's documents and responses to questions, the IAP officer

may recommend to carriers not to board individuals who have documentary deficiencies or who may be otherwise inadmissible.

Additional sites will be identified based on intelligence information, funding, and approval by the Department of Homeland Security and host countries.

Deploying Integrated IDENT/IAFIS

The Automated Biometric Identification System and the Integrated Automated Fingerprint Identification System (IDENT/IAFIS) program was established to integrate the IDENT database with the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS). The Integrated IDENT/IAFIS terminal provides simultaneous access to biometric-based criminal and immigration violator information for DHS agents in the field. In FY2004, DHS assumed the responsibility for funding and completion of phase 1 of the project—the nationwide deployment of IDENT–IAFIS workstations was transferred from the Department of Justice to the Department of Homeland Security (DHS). DHS immediately began accelerating the deployment of the integrated capability and has now completed deployment of the integrated system to all 140 operational Border Patrol stations, and 216 Port of Entry and ICE locations. DHS will complete deployment to all remaining Ports of Entry and ICE locations by December, 2005.

Numerous other initiatives being pursued by CBP include continuing to enhance the automated targeting system, continuing to aggressively pursue smart box container technology, increasing Container Security Initiative (CSI) participation, Free And Secure Trade (FAST), internal law enforcement partnerships, deploying radiation portal monitors, and deploying additional imaging technologies to the ports. Future goals and developing capabilities include our Automated Commercial Environment system (ACE) which is currently restructuring what information is required for international transactions, how that information is processed, and employing technology and business partnerships with other agencies to identify their international data requirements, and how to best integrate these requirements through an international trade data system (ITDS).

QUESTIONS FOR THE RECORD FROM CHAIRMAN DAVE CAMP AND CHAIRMAN JIM GIBBONS

(1) Q02161: What is the current process for DHS agencies to share information and intelligence they gather in their day-to-day activities with the DHS Office of Information Analysis?

Answer: Each Department of Homeland Security (DHS) component employs several methods to share information with the DHS Office of Information Analysis (IA). Standardized, daily reporting is the principal method for sharing information. This regular reporting is supplemented by spot reports, alerts, and informal notifications via email, phone or fax to provide timely notice to IA, and to DHS in general, of emergent threats and other events of interest. The Homeland Security Operations Center (HSOC) is the focal point for this information exchange. IA personnel staff the HSOC on a 24X7X365 basis. This team, under the leadership of the Senior Intelligence Analyst, reviews all component reporting and works directly with both the Senior HSOC Watch Officer and all parts of the IA organization to ensure timely distribution of information throughout IA and to provide front line, first phase intelligence analysis to the HSOC.

Most DHS components provide their reports to the HSOC via email at all classification levels (Sensitive but Unclassified (SBU), Secret (S), and Top Secret/Special Compartmented Information (TS/SCI)). These reports are automatically filed in designated folders accessible across DHS Headquarters for easy access and archival management. The U.S. Coast Guard submits reports in the form of Information Intelligence Report messages to the DoD's Automated Message Handling System (AMHS) and Web Intelligence Search Engine which are both guarded at DHS. In addition, the Coast Guard develops and displays a wealth of information on its Common Operational Picture (COP), and which provides real-time information to the HSOC. That information available through HSOC and through the COP is provided to DHS Office of Internal Affairs (OIA). The following is a listing of reports by agency:

BTS

Daily Operations Report

* BTS components ICE, CBP, and TSA also provide their own reports:

ICE

Homeland Security Intelligence Report

Significant Activity Reports

ICE daily operational summary

ICE Spot Reports
Daily Intelligence Summary

CBP
Homeland Security Intelligence Report
CBP Spot Reports
CBP daily operational summary
Intelligence Assessment
Intelligence Alert
Weekly Matrix

TSA
Daily intelligence Summary
Homeland Security Intelligence Report
Transportation Security Operations Center Spot Reports
Suspicious Incident Report

FAMS
Daily Intelligence Brief
Weekly Assessment

USCG
Coast Guard Incident Reports
Spot Reports
Field Intelligence Reports (via AMHS)
Intelligence Information Reports (via AMHS)
Common Operational Picture
Daily Intelligence Summaries
Routine and ad hoc Intelligence Production

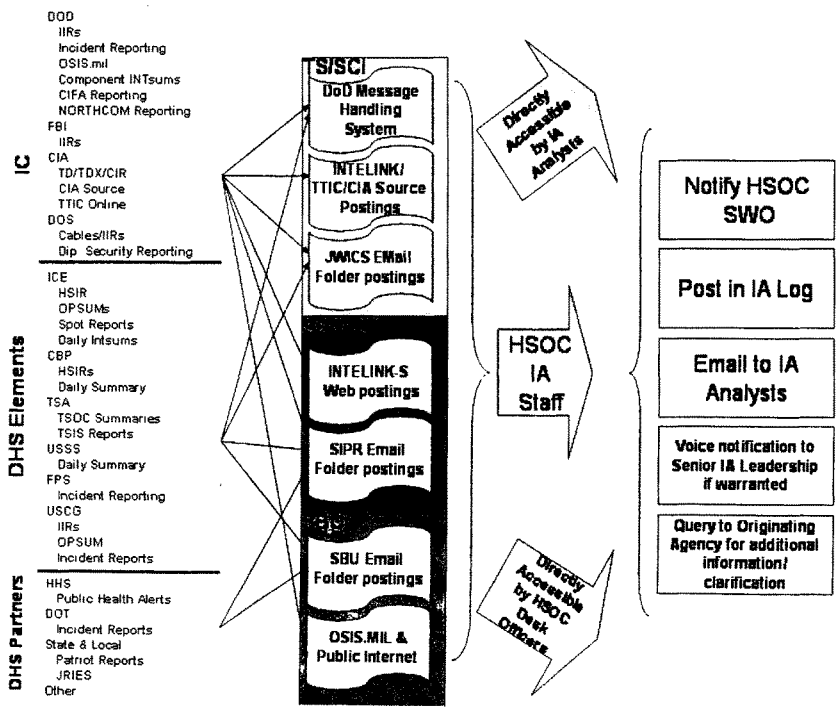
USSS
USSS Intelligence Division/Operations Branch-Daily Operations Report

Federal Protective Service
Daily Operations Log
Spot Reports
Information Bulletins
Incident Reporting via the FPS Portal

This system also supports reporting from DHS affiliates in the National Infrastructure Coordinating Center (NICC). NICC participants are given reporting criteria and email addresses to provide information to the HSOC for further distribution to IA analysts.

The IA staff in the HSOC distributes information through several methods. The report is captured in a running log with the source of the report, the facts as reported, derivation of information gaps, and actions taken to exploit the information against all available databases and subject matter experts to determine terrorism nexus / emergence of threat. External watch officers are often contacted as the information is received, and queried for support in evaluating the threat against their resources. The text of the report is also sent to the HSOC Senior Watch Officer and IA analytic staff via email. If the nature of the information suggests an imminent threat, key IA leaders are notified by phone / pager.

While this process is the primary path of information from components to IA analysts, the same email storage and DoD message systems are available directly to analysts and desk officers with appropriate security clearance. The SIA serves as the primary conduit of information into IA, providing global coverage of all of the over 1500 messages received by DHS daily and ensuring broad distribution of that information on a 24X7 basis, but IA analysts have identical access to the source information for their topic areas to support easy access and rapid analytical response. This process is depicted in the example diagram below:


IC
DHS Elements
DHS Partners
DOD
IIRs
Incident Reporting
OSIS.mil
Component INTsums
CIFA Reporting
NORTHCOM Reporting
FBI
IIRs
CIA
TD/TDX/CIR
CIA Source
TTIC Online
DOS
Cables/IIRs
Dip Security Reporting
ICE
HSIR
OPSUMs
Spot Reports
Daily Intsums
CBP
HSIRs
Daily Summary
TSA
TSOC Summaries
TSIS Reports
USSS
Daily Summary
FPS
Incident Reporting
USCG
IIRs
OPSUM
Incident Reports
HHS
Public Health Alerts
DOT
Incident Reports
State & Local
Patriot Reports
JRIES
Other
TS/SCI
DoD Message Handling System
INTELINK/ TTIC/CIA Source Postings
JWICS EMail Folder postings
INTELINK-S Web postings
SIPR Email Folder postings
SBU Email Folder postings
OSIS.MIL & Public Internet
Directly Accessible by IA Analysts
HSOC IA Staff
Directly Accessible by HSOC Desk Officers
Notify HSOC SWO
Post in IA Log
Email to IA Analysts
Voice notification to Senior IA Leadership if warranted
Query to Originating Agency for additional information/ clarification

Additionally, the DHS Request for Information (RFI) and Tearline process facilitates the sharing of information not only within DHS, but also with members of the Intelligence Community (IC). DHS's Web-based Pantheon system will help expedite and streamline the information sharing process. DHS IA also manages the DHS tearline program that currently helps facilitate information sharing within the IC, DHS, State & Local Government, and the private sector. In response to DCID 8/1, DHS IA has developed a four phased tearline reporting implementation plan which will greatly enhance the ability to share information.

(2) Q02162: Does IA currently have specific personnel devoted to developing a complete threat picture based on information it receives from BTS agencies and the Intelligence Community?

Answer: The Department of Homeland Security (DHS) Office of Information Analysis (IA) currently has two analytical units. One focuses on current intelligence and the other on broader trends and developments. Within the analytic unit focused on current intelligence, there is a branch focused on fusing current intelligence and homeland security reporting, to include DHS Border and Transportation Security (BTS) reporting, with the contextual picture provided by the unit analyzing broader trends and developments. The product of this fusion, along with the near real time input from the Senior Intelligence Analyst in the Homeland Security Operations Center, is a complete threat picture. Additionally, BTS component intelligence activities, as well as representatives from the U.S. Intelligence Community (IC) maintain a presence in IA to facilitate sharing their respective understanding of the current threat picture.

It is the responsibility of IA analysts to be cognizant of and apply knowledge of the broader threat context as derived from all sources of Homeland-related threat information to analyses of their specific accounts or programs. Specific divisions within IA that are focused on information derived from or pertaining to BTS naturally possess a greater macro and micro understanding of this information. It is also the responsibility of senior analysts and managers within IA to ensure all-source fusion is taking place.

Q02163: Is this information integrated with intelligence and reporting from other agencies?

Answer: Yes. Please refer to the above **(Q02162)** and **Q02166.**

(3) In addition to the Office of Information Analysis (IA) within the Department of Homeland Security (DHS), several other components within the Department maintain distinct intelligence units. These units located within the Border and Transportation Security Directorate (BTS) and the U.S. Coast Guard serve the demands of their respective offices.

Q02164: How does IA work with their respective DHS intelligence components to share border reports?

Answer: Please refer to **Q02161.**

Q02165: How is this information shared across the Department, with IA, and with the larger Intelligence Community?

Answer: The Department of Homeland Security (DHS) Office of Information Analysis (IA) utilizes both formal and informal processes to share information across the Department, within IA, and with the larger Intelligence Community. IA conducts and or participates in several daily and weekly meetings/teleconferences. The primary purpose of these events is to discuss and disseminate information/intelligence and assign taskings for further analysis.

The following meetings are of significant importance in the IA information sharing process:

- Information Analysis Morning Executive Brief (IAMEB)—daily Monday through Friday brief that is attended by numerous agencies from DHS to include IA, IP, HSOC, USSS, BTS,CBP,ICE, TSA, State & Local as well as the FBI, State Department and the Intelligence Community.
- Daily Secure Video Teleconference—IA participates in the daily secure meeting hosted by the National Counter Terrorism Threat Center.
- Homeland Security Terrorist Threat Intel Group (HSTTIG)—Bi-monthly meeting of the DHS Intelligence component leaders.

Formal products are produced in a variety of formats to accommodate the different security handling and information requirements of our diverse audience, which ranges from private sector firms and institutions to members of the Intelligence Community.

The department produces a wide variety of formal products including:

- Homeland Security Information Advisories;
- Homeland Security Information Bulletins;

- Homeland Security Assessments and Studies;
- Homeland Security Intelligence Articles (HSIA);
- Homeland Security IAIP Red Cell Session Reports;
- Homeland Security Intelligence Reports;
- Daily briefings such as the Information Analysis Morning Executive Brief;
- Intelligence Information Reports (via DoD message handling system).

Information Advisories (IAs) provide a means for DHS to communicate threat information to all DHS customers ranging from the intelligence community and law enforcement to the general public at large. Advisories incorporate intelligence or information identifying a threat targeting critical national networks or key infrastructure assets that contains actionable incident information. The Advisory may suggest a change in readiness posture, protective actions, or response, as well as, relaying newly developed procedures that, when implemented, would significantly improve security or protection.

Information Bulletins (IBs) report information of interest to the nation's critical infrastructures that does not meet the timeliness, specificity, or significance thresholds of Information Advisories. IBs are designed to provide updates on the training, tactics, or strategies of terrorists and may include: statistical reports, monthly, quarterly, or semi-annual summaries, incident responses or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools. In addition, preliminary requests for information on symptoms, events, or social engineering being observed by constituents may also be communicated through a bulletin.

Homeland Security Assessments and Studies provide an assessment or study for a specific event or location and are directed at a specific audience. Assessments are typically 2~5 pages, while Studies offer a more in-depth coverage of the subject and are typically 10~20 pages in length. These come in various forms including: Threat—particular event related; Special—study of threats to infrastructure / security; Executive—summary assessments; and Joint—author sponsorship by DHS and another concerned organization.

Homeland Security Information Articles (HSIAs) are classified, timely, all-source intelligence products that assess, clarify or consolidate new intelligence with previously reported information. HSIAs are an analytic production process that begins with new intelligence or threat information often expanding upon previously reported intelligence and threat assessments. The information is not limited to raw reporting and may contain finished analysis. The HSIA is authored by IA–C and/or IA–D analysts on an as-needed basis and is intended for various internal DHS audiences and the Intelligence Community.

IAIP Red Cell Reports provide alternative assessments intended to provoke thought and stimulate discussion. Red Cell products enhance DHS analysis by engaging a community of outside experts from government, industry, and academia to provide an alternative perspective on threats/vulnerabilities facing the homeland. Emphasis will be is on examining issues from a terrorist mindset, focusing on innovative and unconventional targets and tactics. The analytic Red Cell program brings together DHS and outside experts on a regularly scheduled basis, and can also stand up ad-hoc red cells in response to immediate needs. Distribution is generally limited based on topic.

Homeland Security Intelligence Reports (HSIRs) allow DHS operational components a vehicle to report case and potential terrorist information to DHS Headquarters. The final report contains a compilation of information with preliminary processing or analysis by the reporting agency supported by research using locally available databases and domain expertise of the component analysts.

Information Analysis Morning Executive Brief (IAMEB) provides daily situational awareness on homeland security issues. The brief is a daily compilation of preliminary/ in-depth analytical perspectives on significant recent and developing issues affecting homeland security and DHS. The IA–C briefing team develops the IAMEB with input from IA–D as warranted, and briefs it to key IAIP personnel each weekday morning. The IAMEB is then modified as appropriate and disseminated. Appropriate versions of the IAMEB are sent internally throughout DHS and the Intelligence Community.

DHS Intelligence Information Reports (IIRs) are produced by IA to publish information gathered by DHS components in the format most familiar to IC and DoD consumers. IA has partnered with DIA to allow direct publication of DHS IIRs into the standard DoD message handling system. Currently, DHS authors' component reporting in this format, however, components will begin production on their own to directly inject the information into the IC in the near future.

Homeland Security Information Message (HSIM): Designed to communicate uncorroborated threat information to U.S. Government agencies, State and Local Homeland Security Advisors, and/or the private/public sector, in an expeditious

manner. Information has not been fully evaluated. No specific actions are recommended. Should further information become available, it will be disseminated as a more comprehensive Information Bulletin, Advisory or Memorandum.

This information is provided as directed in Section 201, Homeland Security Act of 2002. Additionally, IA is in constant informal communication with other Intelligence agencies and other non-intelligence organizations, directly communicating information via liaison, phone, fax or e-mail. We rely heavily on representatives of the various agencies, both inside and outside DHS, to facilitate communication with their parent organizations. These experts provide not only a conduit for information, but also are valuable resources during the development and vetting of products.

(4) Q02166: Does IA have the ability to analyze imagery and other forms of telligence that is gathered on our borders?

Answer: Analyzing and consuming all-source intelligence analysis is at the core of the Department of Homeland Security (DHS) Office of Information Analysis (IA) mission. However, IA does not literally analyze imagery, with the exception of a small contingent of imagery analysts working within the Coast Guard who provide analysis of maritime events that impact a wide variety of USCG missions. However, for the most part, IA relies on the analysis of the National Geospatial Intelligence Agency (NGA) and other organizations that possess literal imagery analysts. This analysis is incorporated into IA evaluations and assessments pertaining to border issues. As a member of the U.S. Intelligence Community, NGA maintains multiple representatives within IA who very ably assist with various imagery requirements. Most notably, NGA has played a key role supporting DHS Information Analysis and Infrastructure Protection (IAIP) Directorate efforts relating to critical infrastructure protection, and has supported IAIP's mission to National Security Special Events and other significant functions. Other border-related information derived from the IC or BTS is funneled to DHS via established electronic systems and incorporated into IA's assessments.

(5) Terrorist travel intelligence runs across broad federal, state, and local agency lines.

Q02167: How is the Department leveraging its assets to best utilize current terrorist travel information from within DHS and other partners in the Intelligence Community?

Q02168: What is it doing to improve the exchange of information?

Answer: One of IA's OMB Milestones is to "Establish and resource a DHS reports officer capability to report information from field and component organizations on potential threats to the Homeland." IA is staffing positions, developing procedures and training, and implementing a plan to deploy reports officers to the field. These reports officers' primary responsibility is to write and disseminate reports of intelligence value based on DHS component operational information. IA's intent is to model this effort on successful reports officer programs of long standing in the Intelligence Community and to review the newly developed program at the FBI for lessons learned in a start-up enterprise.

LAWRENCE M. WEIN RESPONSES TO QUESTIONS FROM CHAIRMAN DAVE CAMP AND CHAIRMAN JIM GIBBONS

Thank you for the opportunity to testify before the Select Committee on Homeland Security Subcommittees on Infrastructure and Border Security and Intelligence and Counterterrorism hearing on September 30, 2004, entitled "Disrupting Terrorist Travel: Safeguarding America's Borders through Information Sharing." I am pleased to answer your questions.

Question 1: You make the point in your testimony that the more fingerprints captured, the less important image quality is. However, if I'm a terrorist I can just as easily ruin or impair all 10 of my fingerprints as I can just two. How do you make the assumption that 10 prints are essential?

Answer 1: First, approximately 5–10% of terrorists have poor image quality in the absence of any deliberate impairment. Given Al-Qa'ida's large pool of terrorists, it can simply choose US-bound terrorists that have inherently poor image quality. Second, approximately five times as much work, pain, etc. is required to impair 10 fingers rather than two fingers, although your point is well taken that terrorists who are capable of deliberately impairing two fingers can certainly deliberately impair 10 fingers. Regarding your main question, the bottom line here is that you get a limited amount of information out of a fingerprint with poor image quality, and you get approximately five times as much information from 10 poor-quality fingerprints as you do from two poor-quality fingerprints. We do not *assume* that 10 fingerprints are essential. Rather, we solve an optimization problem that allows for the

possible use of up to 10 fingerprints, and find that it is optimal to employ 10 fingerprints from visitors with poor-quality fingerprint images. That is, the use of 10 fingerprints for visitors with poor image quality is not an assumption of our analysis, but rather a product of our analysis. Returning to the earlier issue, using 10 fingerprints allows five times as much information to be captured from visitors with inherently, or deliberately, poor image quality, which leads to a much higher detection probability.

Question 2: What factors are involved in order to capture a quality image? (i.e., capabilities of the machine, software, screener training, and physical characteristics of the fingers).

Question 3: It seems that if US VISIT is capturing quality images, the matching problems you outline in your testimony will largely be addressed. In your estimate, how much of the ability to capture a quality image is outside of DHS's control?

Answers 2 and 3: While all the factors you mention in Question 2—along with environmental factors such as humidity and dirt—impact image quality, our analysis of the data in Figure 11 of the NISTIR 7110 report (this analysis appears in Appendix I of a report we distributed to various parts of the US Government, including analysts at NIST and managers of the US-VISIT Program) suggests that most of the image quality is inherent in the physical characteristics of the person (i.e., some people have inherently worn-out fingers), and hence is outside of DHS's control. However, a definitive answer to this question requires an analysis of NIST data that is more detailed than the summary statistics in Figure 11 of NISTIR 7110; I requested this additional data from NIST analysts on June 2, 2004, but they never responded to my request.

Question 4: You concluded in your testimony that capturing additional fingerprints would not take additional time because you average the screening time between primary and secondary. Your findings combine the time in primary and secondary into a mean time. I am concerned that your findings don't fully weigh the cost of delaying travelers at a port of entry. **What are you recommending exactly—that 10 fingerprints are captured during primary inspection at the port of entry or at some other point in the screening process?**

Answer 4: We are also concerned with traveler delay at ports of entry. Unlike most previous biometric research, our analysis includes a constraint that the total mean (primary plus secondary) screening time per visitor be fixed at its current value. Queueing theory, which is the field of mathematics that analyzes waiting lines (see our report for a reference to a specific paper) implies that mean delay at ports of entry will not increase if the mean (primary plus secondary) screening time per visitor is not increased, under the assumption that there is some flexibility in the workforce (i.e., a small fraction of the inspectors are trained in both primary and secondary screening). Hence, we are taking traveler delay into full consideration. Regarding your final question, our recommendation is that 10 fingerprints be captured during visa enrollment from all during their next visit to a port of entry, and these 10 prints could replace the 2 fingerprints that were originally captured during enrollment. Our exact recommendation at the ports of entry is to take 10 fingerprints from enrollees with poor image quality, but only two fingers from the enrollees with good image quality. Using this information to match against the watchlist, we predict a detection probability of 95% with no increase in mean traveler delay. Of course, if different numbers of fingerprints are captured from different people, there is the issue of managing the perception of differential treatment (i.e., different numbers of fingers for different people). However, image quality is an objective measure that does not explicitly take into account age, gender, race, country of origin, etc., which may mitigate this concern.

Question 5: I am concerned about the additional burden and time delay of taking 10 fingers from all travelers. Did you assess what the added value would be of taking 10 prints from all enrollees with poor image quality, as a subgroup of all visitors?

Answer 5: This question was essentially answered in Answer 4, but I will repeat the answer here. We are also concerned with the time delay of taking 10 fingers from all travelers. In fact, in our analysis, 95% detection probability at the port of entry (with no increase in traveler delay) is achieved by taking 10 fingerprints from enrollees with poor image quality, but only two fingers from the enrollees with good image quality; note that we would know an enrollee's image quality from their prints taken at the time of enrollment. Of course, if different numbers of fingerprints are captured from different people, there is the issue of managing the perception of differential treatment (i.e., different numbers of fingers for different people).

However, image quality is an objective measure that does not explicitly take into account age, gender, race, country of origin, etc., which may mitigate this concern.

Thank you for your interest. Please let me know if I can be of any further help.

Mr. CAMP. The gentleman from Texas.

Mr. TURNER. Mr. Chairman, I just wanted to ask the chairman if he would allow me to place in the record a NIST 2002 report, which concluded that the addition of the additional fingerprint slap system that I believe you were referring to, Professor, the time required to capture those fingerprints would be insignificant.

It goes to the heart of the issue that Mr. Dicks raised, because I think we all have the impression that we didn't use the 10-print system because it takes too much time. And I would like for this report to be placed as part of the record of this hearing.

Mr. CAMP. Without objection, the NIST report may be placed in the record.

[Retained in the committee file.]

Mr. CAMP. There being no further business, the hearing is now adjourned.

[Whereupon, at 3 p.m., the subcommittee was adjourned.]

○