# ELEVEN YEARS LATER: PREVENTING TERRORISTS FROM COMING TO AMERICA

## HEARING

BEFORE THE

## SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

OF THE

## COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

SEPTEMBER 11, 2012

**Serial No. 112–113**

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

80–855 PDF WASHINGTON : 2013

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

## COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
RON BARBER, Arizona

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

---

## SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

CANDICE S. MILLER, Michigan, *Chairwoman*

MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
PAUL C. BROUN, Georgia
BEN QUAYLE, Arizona, *Vice Chair*
SCOTT RIGELL, Virginia
JEFF DUNCAN, South Carolina
PETER T. KING, New York *(Ex Officio)*

HENRY CUELLAR, Texas
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
BRIAN HIGGINS, New York
HANSEN CLARKE, Michigan
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

PAUL ANSTINE, *Staff Director*
DIANA BERGWIN, *Subcommittee Clerk*
ALISON NORTHROP, *Minority Subcommittee Director*

# CONTENTS


Page

STATEMENTS

The Honorable Candice S. Miller, a Representative in Congress From the State of Michigan, and Chairwoman, Subcommittee on Border and Maritime Security:
Oral Statement ..... 1
Prepared Statement ..... 3
The Honorable Henry Cuellar, a Representative in Congress From the State of Texas, and Ranking Member, Subcommittee on Border and Maritime Security ..... 4

WITNESSES

Ms. Kelli Ann Walther, Deputy Assistant Secretary, Office of Policy, Department of Homeland Security:
Oral Statement ..... 6
Prepared Statement ..... 8
Mr. Kevin McAleenan, Acting Assistant Commissioner, Office of Field Operations, Customs and Border Protection, Department of Homeland Security:
Oral Statement ..... 16
Prepared Statement ..... 17
Mr. John P. Woods, Assistant Director, National Security Investigations, Homeland Security Investigations, Immigrations and Customs Enforcement, Department of Homeland Security:
Oral Statement ..... 23
Prepared Statement ..... 24
Mr. Edward J. Ramotowski, Deputy Assistant Secretary, Bureau of Consular Affairs, U.S. Department of State:
Oral Statement ..... 29
Prepared Statement ..... 30
Mr. Charles K. Edwards, Acting Inspector General, Office of the Inspector General, Department of Homeland Security:
Oral Statement ..... 36
Prepared Statement ..... 37

APPENDIX

Questions From Ranking Member Bennie G. Thompson for Kelli Ann Walther ..... 45

# ELEVEN YEARS LATER: PREVENTING TERRORISTS FROM COMING TO AMERICA

**Tuesday, September 11, 2012**

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY,
*Washington, DC.*

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 311, Cannon House Office Building, Hon. Candice S. Miller [Chairwoman of the subcommittee] presiding.

Present: Representatives Miller, Duncan, Cuellar, Jackson Lee, Higgins, and Clarke.

Mrs. MILLER. Good morning, everyone. The Committee on Homeland Security, Subcommittee on Border and Maritime Security will come to order. The subcommittee is meeting today to examine the Department of Homeland Security's ability to prevent terrorists from traveling to the United States.

We have an excellent panel of witnesses. I would just remind the committee, though, and the witnesses as well, obviously in remembrance of this day, 9/11, 11 years ago, we have some pictures on the back of this committee room which remind us all, each and every day, of why this committee was even formed, the main committee and certainly our subcommittees as well.

There will be a commemorative ceremony at 11:00 o'clock today. All the Members of Congress will be gathering, the House and the Senate, at the East Center Staircase for the Congressional Remembrance Ceremony marking the observance of September 11, 2001.

So this committee will be certainly joining our other colleagues. We will have opening statements from myself and our Ranking Member and the statements of our witnesses. We will see where we are on time, because we will have a hard break probably at about 10 to 11:00 for folks.

Our witnesses today are Kelli Ann Walther, who is the deputy assistant secretary for policy at the Department, Kevin McAleenan, acting assistant commissioner in the Office of Field Operations at Customs and Border Protection, John Woods, assistant director for national security investigation at ICE, Ed Ramotowski, deputy assistant secretary for visa services at the Department of State, and Charles Edwards, the acting inspector general at the Department of Homeland Security.

Eleven years ago today, 19 terrorist cowards successfully penetrated our border and visa security defenses and hijacked four planes to conduct a terrible, terrible attack against nearly 3,000 innocent people. That act of violence, as I said, is the very reason the

Department of Homeland Security exists, and why this committee was created to prevent another terrorist attack on our homeland.

We should never forget, of course, what happened on that Tuesday in September when so many of our fellow Americans died tragically, or fail to remember the first responders as well, all of the victims of that tragedy. One of the ways I think that we can honor those who lost their lives that terrible day is to make sure an attack like that never happens again, to harden our defenses and to take into account the hard lessons that we learned that day.

Among the most important weaknesses the attackers exploited was the porous outer ring of border security. The hijackers actually passed through United States Border Security a combined total of 68 times. The relative ease with which the terrorists evaded detection by presenting fraudulent documentation, passports, and made detectable false statements on visa applications, gave false statements to border officials, and certainly the failure to watch lists with known al-Qaeda operatives became missed opportunities to stop those attacks.

It has highlighted certainly the need to close the holes exploited by the 9/11 terrorists by strengthening our border security and visa issuance policy. Curtailing the ability of terrorists to travel to the United States can be one of the most effective counter-terrorism tools, because denying terrorists the freedom to travel essentially eliminates their ability to plan or to exercise or to carry out attacks on our homeland.

As the 9/11 Commission Report noted, said in the report, for terrorists, travel documents are as important as weapons, which is a very interesting statement I think. Building on that key insight, we strengthen our outer ring of border security to conduct more rigorous checks, collect biometric data and continuously check visa holders against the terrorist watch list.

We have pushed our border out by conducting more checks overseas before passengers even board an airplane or present themselves to a CBP officer at any of our ports of entry, a layered approach that increases our chances of preventing terrorists from ever coming to America.

Today, we collect more information on foreign travelers that allows CBP, through the National Targeting Center, to use complex targeting rules which examine travel patterns, allowing agents to find any problems with travel documents that might raise a red flag.

Programs such as CBP's Immigration Advisory Program and ICE's Visa Security Unit, that stations officers and agents overseas, are critical components of our success at keeping those with terrorism links and other high-risk passengers off planes that are bound into the United States.

Without question, we have made enormous progress, limiting the ability of terrorists to travel to the United States since 9/11. But certainly the incident of the Christmas day bomber, that demonstrated that we still have some significant gaps in our visa vetting system.

Continually vetting visa and electronic systems for travel authorization holders against our watch list is a welcome improvement, but we are going to be interested from hearing from our witnesses

today how we can further leverage the power of targeting systems to vet visa applicants before a visa is ever issued.

Improvements to watch listing processes have increased the ability of consular officers and other border security officials to keep those individuals that concern us out of the country. But we still need to do better.

So we will be interested again to hear from the witnesses on how we vet visa applicants that are known to the intelligence community, and how we resolve visa issuance through the Security Advisory Opinion Process.

Unlike several of this subcommittee's previous hearings where we discussed the challenges of tracking down visa over-stays and the delay in rolling out a reliable exit system that allows Department of Homeland Security to determine if a visa holder has departed in accordance with the terms of their visa, this hearing is really focused on the front end of the visa process.

We certainly believe that a viable exit system, of course, is vital to our National security efforts. But it is incumbent on the Department of Homeland Security and the Department of State to also focus their efforts on preventing terrorists from coming into the country in the first place.

Also look forward to hearing from the inspector general in regards to their recent work which identified challenges with US–VISIT and the multiple names associated with the same set of fingerprints, a gap certainly that needs to be swiftly corrected to prevent fraud and exploitation by any terrorist.

Certainly contrary to what some have suggested, al–Qaeda, although diminished in capability thanks to the wonderful work, heroism, and professionalism and bravery of our men and women in uniform and our allies, still, they are a lethal enemy intent on attacking the homeland.

Vigilance is certainly one of the best tools at our disposal to prevent terror travel. So that is why we are here today, to examine those gaps, vulnerability in the visa immigration system, and how they have been addressed in the period since 9/11.

[The statement of Chairwoman Miller follows:]

STATEMENT OF CHAIRWOMAN CANDICE S. MILLER

Eleven years ago today, 19 men successfully penetrated our border and visa security defenses and hijacked four planes to conduct a heinous attack against nearly 3,000 innocent people.

That act of violence is the very reason the Department of the Homeland Security exists, and why this committee was created—to prevent another terrorist attack on the homeland.

Along the walls, we have photographs of the aftermath of those attacks to remind us why we're here—and most importantly the cost of failure.

We should never forget what happened on that Tuesday in September to so many of our fellow Americans, or fail to remember the first responders and victims of that tragedy.

I would like to ask you to join me in a moment of silence in honor of those who died in the World Trade Center and the Pentagon.

One of the ways we can honor those who lost their lives is to make sure an attack like that never happens again—to harden our defenses and take into account the hard lessons learned from that horrible day.

Among the most important weaknesses the attackers exploited was the weakness of our "outer ring of border security." The hijackers passed through U.S. border security a combined total of 68 times.

The relative ease with which the terrorists evaded detection by presenting fraudulent documents and passports with suspicious indicators, made detectable false statements on visa applications, gave false statements to border officials, and the failure to watchlist known al-Qaeda operatives became missed opportunities to stop the attacks.

It highlighted the need to close the holes exploited by the 9/11 terrorists by strengthening our border security and visa issuance policy because curtailing the ability of terrorists to travel to the United States can be one of the most effective counterterrorism tools.

Denying terrorists the freedom to travel essentially eliminates their ability to plan, exercise, and carry out attacks on the homeland.

As the 9/11 Commission Report noted, "For terrorists, travel documents are as important as weapons." Building on that key insight, we have strengthened our "outer ring of border security" to conduct more rigorous checks, collect biometric data, and continuously check visa holders against the terror watch lists.

We have pushed our border out by conducting more checks overseas before passengers board a plane, or present themselves to a CBP officer at the port of entry—a layered approach that increases our chances of preventing terrorists from ever coming to America.

Today, we collect more information on foreign travelers that allows CBP, through the National Targeting Center, to use complex targeting rules, which examine travel patterns—allowing agents to discern problems with travel documents that might raise red flags.

And programs, such as CBP's Immigration Advisory Program and ICE's Visa Security Units, that station officers and agents overseas are critical components of our successes in keeping those with terrorism links and other high-risk passengers off planes bound for the United States.

Without question, we have made progress limiting the ability of terrorists to travel to the United States since 9/11, but the Christmas day bombing attempt demonstrated there are still significant gaps in our visa vetting system.

Continually vetting visa and Electronic System for Travel Authorization (ESTA) holders against our watch lists is a welcome improvement, but I will be interested in hearing from our witnesses on how we can further leverage the power of targeting systems to vet visa applicants before a visa is ever issued.

Improvements to watch-listing processes have increased the ability of consular officers and other border security officials to keep those individuals that concern us out of the country, but I am still concerned that being on a watch list is not an automatic bar to getting a visa.

I will be interested to hear from the witnesses on how we vet visa applicants that are known to the intelligence community, and how we resolve visa issuance through the Security Advisory Opinion process.

Unlike several of this subcommittee's previous hearings, where we have discussed the challenges of tracking down visa overstays, and the delay in rolling out a reliable exit system that allows DHS to determine if a visa holder has departed in accordance with the terms of their visa, this hearing is focused on the front end of the visa process.

I continue to believe that a viable exit system is vital to our National security efforts, but it is incumbent on DHS and the Department of State to also focus their efforts on preventing terrorists from coming to the country in the first place because it is much easier to detect them on the front end of the process.

I also look forward to hearing from the DHS Inspector General in regards to their recent work which identified challenges with US–VISIT, and the multiple names associated with the same set of fingerprints—a gap that needs to be swiftly corrected to prevent fraud and the exploitation by terrorists.

Contrary to what some have suggested, al-Qaeda, although diminished in capability, is still a lethal enemy, intent on attacking the homeland. Vigilance is one of the best tools at our disposal to prevent terror travel.

That is why we are here today—to examine how gaps and vulnerabilities in the visa and immigration system have been addressed in the period since 9/11.

I look forward to hearing from the distinguished panel of witnesses and with that I'll yield to the Ranking Member.

Mrs. MILLER. The Chairwoman now recognizes the Ranking Member for his opening statement.

Mr. CUELLER. Thank you, Madam Chairwoman. I join Chairwoman Miller and my colleagues in remembering those who lost their lives in the terrorist attacks of September 11, 2001. Our

thoughts and our prayers are with them and their families today, the 11th anniversary of this tragedy. Of course, every day our prayers are with them.

One way we can honor those who died is to do our utmost to prevent terrorists from traveling to countries to do us harm. The 9/11 hijackers did not sneak into the country across our land borders, but rather entered the United States via an airplane and carrying visas.

The attempted bomber of an airline on Christmas day, 2009, was a stark reminder of the vulnerabilities in the visa process. The Department of Homeland Security and the Department of State, with the direction of Congress, have taken important steps to strengthen visa security and to pre-screen air passengers traveling to the United States.

With DHS, the U.S. Immigration, Customs Enforcement—ICE—has expanded its Visa Security Program at our overseas embassies, providing an important additional layer of security in visa securities and security matters.

Similarly, the U.S. Customs Border Protection has deployed Immigration Advisory Program officers at foreign airports and strengthened its ability to identify travelers of concern bound for the United States. CBPS also enhances efforts at the National Targeting Center to combat terrorist travel.

These programs require investments in personnel, technology, and resources. So it is imperative that Congress continues providing DHS the funding it needs to carry out its mission.

Today, I look forward to hearing about what security enhancements have been made since the subcommittee met last year on this important issue, as well as what remains to be done.

A related issue that I continue to find troubling is that of recalcitrant countries. It is my understanding that certain individuals subject to orders of removal from the United States are often delayed due to their respective Government's refusal to accept the return of their nationals or use lengthy delay tactics.

I have raised this issue in previous hearings. I appreciate the difficult and delicate nature of this issue. But we must address this issue. We, the Chairwoman and I and the committee, look forward to working with you on this issue.

However, I look forward to hearing more from the Department and ICE about recommended steps for improvements. So any steps you all might have, any ideas that you might have, please work with our committee.

I certainly thank Chairwoman Miller for having this particular hearing, her leadership. I appreciate all the witnesses for joining us here. I look forward to your testimony.

I yield back the balance of my time.

Mrs. MILLER. I thank the gentlemen. The other committee Members are reminded that any opening statements they may have can be entered into the record.

What I will do is introduce each one of the witnesses. Then we will start over here. Give a short bio here.

First of all, as I mentioned, we are joined by Ms. Kelli Ann Walther, who currently serves as the senior director for the Department of Homeland Security Screening Coordination Office. Ms.

Walther began working in the SCO in 2007, where she is currently responsible for setting policy and direction that harmonizes a variety of Department of Homeland Security screening programs and investments.

Mr. Kevin McAleenan is the acting assistant commissioner at the U.S. Customs and Border Protection, where he is responsible for overseeing CBP's anti-terrorism, immigration, anti-smuggling, trade compliance, and agricultural protection operations at 20 major field offices, 331 ports of entry, and 70 locations in over 40 countries internationally.

Mr. John Woods is the assistant director at U.S. Immigration and Customs Enforcement, where he oversees National Security Investigations Division within Homeland Security Investigations. As chief of this 450-person headquarters division, he manages a $160 million operational budget and overseas HSI's investigative, regulatory, and technological programs, targeting transnational National security threats arising from illicit travel, trade, and financial enterprises.

Mr. Ed Ramotowski is a deputy assistant secretary for visa services at the United States Department of State. In this position, he oversees the visa office in Washington, DC, two domestic processing centers, as well as visa operations at over 200 U.S. embassies—excuse me—and consulates abroad. He has previously worked as a special assistant to the assistant secretary of state for consular affairs, chief of the consular section at the U.S. Embassy in Nassau, Bahamas, as the U.S. consul in Warsaw, Poland, as well.

Mr. Charles Edwards is the acting inspector general of the Department of Homeland Security. He has over 20 years of experience in the Federal Government and has held leadership positions at several Federal agencies, including the Transportation and Security Administration, the U.S. Postal Service's Office of Inspector General, and the United States Postal Service.

The Chairwoman would now recognize Ms. Walther for her opening testimony.

**STATEMENT OF KELLI ANN WALTHER, DEPUTY ASSISTANT SECRETARY, OFFICE OF POLICY, DEPARTMENT OF HOMELAND SECURITY**

Ms. WALTHER. Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee, thank you for the opportunity to highlight our work on preventing terrorist travel. I head the Screening Coordination Office, where we facilitate policy decisions for people screening programs, from planning through implementation.

We are the DHS coordination point for inter-agency screening initiatives as well. As the 9/11 Commission pointed out, targeting terrorist travel is one of the most powerful weapons we have to counter terrorist operations. Today's threat environment is complex and multifaceted. So it is imperative we employ layers of security throughout the travel continuum, to identify individuals that may pose a risk before they reach the United States.

We recognize there is no one-size-fits-all approach to security. Our approach includes close coordination with counter-terrorism,

law enforcement and public security authorities, the private sector and our State, local, Tribal, territorial, and foreign partners.

To support these efforts, DHS collects biographic and biometric data for screening against various databases to track known threats. We utilize intelligence-based targeting rules and risk-based screening to better identify unknown threats.

A risk-based approach is the foundation of the DHS model today, and in a more comprehensive and sophisticated form than ever before.

With the advent of better information technology, DHS has been able to apply this approach across the life cycle of a traveler's journey, including first when a traveler seeks an authorization to travel, either a visa or ESTA; second just prior to travel, when DHS conducts passenger manifest and reservation screening; third, when a person seeks to board a commercial aircraft or vessel, passengers must undergo physical screening; and finally upon arrival at a port of entry, when a traveler seeks admission to the United States, DHS conducts verification of a traveler's identity and identity documents.

Today, the visa waiver program is more robust than ever before, with strengthened international partnerships and enhanced information-sharing arrangements. Today, we receive data we never had access to before. We now conduct ESTA checks on every VWP traveler.

In the last 3 years, DHS has also achieved a major aviation security milestone by assuming responsibility for terrorist watch list screening for all aircraft operators covered by the Secure Flight final rule. Today, Secure Flight vets 100 percent of all commercial airline passengers flying into, out of, and within the United States—approximately 2 million passengers every day.

We know that implementing such secure measures must be done while ensuring the facilitation of legitimate trade and travel. Trusted traveler programs such as Global Entry include over 1.4 million pre-approved low-risk travelers who may undergo expedited inspection.

These individuals are our most frequent border-crossing travelers. Because they are known, they usually enter the United States in a fraction of the time of other individuals. Additionally, TSA has implemented its Pre-Check Expedited Screening Program. TSA Pre-Check uses intelligence-driven information and a risk-based approach to provide more effective screening, focusing resources on those travelers we know the least about, while providing expedited screening and a better experience for travelers we know the most about.

In the past 10 years, we have made great strides to facilitate the known traveler, leaving us more time to identify the unknown threat. But let me be clear, no visa, ESTA, trusted traveler program provides carte blanche to enter the United States. Throughout all the phases of travel, DHS is constantly monitoring changes to the watch list that could lead to recommendations against boarding or revocation of a visa, refusal of admission, or even removal of an individual.

DHS mitigates risks in a way that effectively establishes and uses security measures to promote the safe movement of people

and commerce, while respecting privacy, civil rights and civil liberties. With this in mind, DHS is also deliberate in its efforts to provide travelers an opportunity to be heard.

The DHS Traveler Redress Inquiry Program, or DHS TRIP, is a single point of contact for individuals, regardless of citizenship, who have inquiries or seek resolution of difficulties they experience during travel.

Today, in response to 9/11 and evolving threats, we have significantly adapted and enhanced our ability to detect travel threats at the earliest opportunity. DHS does not work alone in this mission.

Terror screening is a multi-agency and collaborative effort. More work remains to be done.

But Chairman Miller, Ranking Member Cuellar, I can assure you that the men and women of the Department of Homeland Security never forget. Our goal is to keep the country safe. For us, it is not a job. It is a mission.

Thank you for this opportunity to update the committee on the progress the Department has made in recent years. Thank you for holding this hearing.

I have submitted written testimony and respectfully request it be made part of the hearing record. I look forward to your questions.

[The prepared statement of Ms. Walther follows:]

PREPARED STATEMENT OF KELLI ANN WALTHER

SEPTEMBER 11, 2012

INTRODUCTION

Good morning Chairman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee. Thank you for the opportunity to appear before the subcommittee to highlight the Department of Homeland Security's (DHS) work in preventing terrorist travel.

Eleven years ago, screening of passengers coming to the United States was limited to the Department of State (DOS) visa process, if applicable, the inspection of a person by an immigration officer at the port of entry, and processes applied at foreign airports by foreign governments. Provision of advance passenger information was voluntary and, even when provided by air carriers, frequently contained inaccurate or inconsistent data. There was no biometric collection for visa applicants beyond photographs, or from aliens seeking admission to the United States. There was limited pre-departure screening of passengers seeking to fly to the United States, virtually no screening of any kind for domestic flights beyond the security checkpoint, and no advance vetting of passengers seeking admission under the Visa Waiver Program (VWP). Interagency sharing of information on terrorist threats was minimal.

Today, in response to both 9/11 and evolving threats, and with the help and support of Congress, we have significantly adapted and enhanced our ability to detect and interdict threats at the earliest opportunity. As the 9/11 Commission pointed out, targeting terrorist travel is one of the most powerful weapons we have to counter terrorist operations. One of the key aspects of the DHS approach is to identify persons that may pose a risk to U.S. citizens or whose entry may violate U.S. law, before they reach the United States.

DHS works to track known threats, while utilizing intelligence-based advanced targeting techniques to help mitigate and identify unknown threats. For example, DHS uses the U.S. Government's consolidated terrorist watch list and other information derived from investigations and intelligence assets to identify individuals with known or suspected ties to terrorism and other potential threats to the United States. In addition, DHS relies on domestic and international criminal records (e.g., investigative case files domestically and INTERPOL notices internationally) to identify potential criminal movements. Travel data is also compared against passport, visa, and immigration data to determine if travelers are admissible or can enter the United States. Moreover, DHS implements rigorous physical security requirements

both in the form of airport checkpoint and airline security standards, as well as physical detection methodologies (e.g., drug-sniffing canines) at ports of entry.

Identifying travelers through a risk-based approach remains the foundation of the DHS model today, and in a more comprehensive and sophisticated form than ever before. With the advent of better information technology within Government and the transportation industry, DHS has been able to apply this methodology across the life cycle of a traveler's journey.

## DHS'S MULTI-LAYERED APPROACH TO SECURITY

Since 9/11, the travel threat has evolved to include not only large-scale attacks, but also smaller operations with potentially catastrophic effects. Our approach employs multiple layers of security measures throughout the travel continuum that are closely coordinated with other U.S. Government counterterrorism, law enforcement, and public security authorities and with State, local, Tribal, territorial, and foreign partners and the transportation industry. To support these efforts, DHS collects biographic and biometric data for vetting and screening against various databases to track known threats and better identify and mitigate unknown threats.

This multi-layered approach allows DHS to improve security and to minimize the likelihood that any single measure becomes a single point of failure.

### *Enhancements Since December 25, 2009*

Since the attempted bombing of a commercial aircraft on December 25, 2009, DHS, in coordination with other departments and agencies, has worked to address issues and potential gaps to ensure that we have a comprehensive and multi-layered approach that focuses on stopping terrorists at the earliest possible opportunity. As represented by the other officials who have been asked to testify today, we can see that addressing this issue requires significant collaboration and coordination among Federal agencies.

Our efforts are not all directed at one area of the travel continuum—but rather are part of our layered approach to strengthen security. Working in concert with other U.S. agencies, DHS has strengthened security, law enforcement, and screening at several points in the travel process:

- During the travel planning phase, when a traveler seeks a visa or authorization to travel;
- Just prior to travel, when a person seeks to board a commercial carrier or vessel;
- Upon arrival at a port of entry, when a traveler seeks admission into the United States;
- During the period of stay in the United States, when a non-U.S. person travels by air within the United States; and
- Upon departure, when a traveler leaves the United States.

DHS, in cooperation with commercial carriers and vessels, reviews information about travelers, including their identity and travel documents, prior to arrival at a U.S. port of entry. The traveler establishes his or her identity through the provision of biographic and biometric data, which is confirmed at various points in the travel continuum.

## SCREENING IN THE TRAVEL PLANNING PHASE

This layer of defense consists of deploying safeguards to prevent dangerous individuals from obtaining visas and travel authorizations. To enter the United States, most foreign nationals are required to either obtain a visa issued by a U.S. embassy or consulate or, for citizens or nationals of a Visa Waiver Program (VWP) country,[1] obtain a travel authorization via the Electronic System for Travel Authorization (ESTA). Visa applicants are required to provide biometric (fingerprint and digital photo) and biographic data. The applicant's information is checked against the biometric and biographic databases of DHS, DOS, and the Federal Bureau of Investigation. In most instances, individuals must also appear in-person for an interview with a consular official.

DHS is continually working with interagency stakeholders to improve procedures for vetting immigrant and nonimmigrant visa applicants, asylum applicants, and refugees. The interagency vetting process in place today is more robust and con-

[1] The 36 countries currently designated for participation in the Visa Waiver Program include: Andorra, Australia, Austria, Belgium, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, South Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

siders a far broader range of information than it did in past years. Visa applicants, asylum applicants, refugees, and those seeking to enter the United States at a port of entry, are subject to rigorous background vetting, biographic, and biometric checks. The security procedures for all of these categories have been enhanced over the past several years as vetting capabilities have evolved and interagency partnerships with the law enforcement and intelligence communities have been strengthened.

By continuously vetting all issued U.S. non-immigrant visas against law enforcement data, changes in a traveler's eligibility are identified by DHS in near real-time, allowing DHS to submit timely "no-board" recommendations to carriers, visa revocation requests to DOS, or notifications to other law enforcement agencies in situations where the individual is physically present in the United States.

In an effort to identify potential terrorists and criminals before they obtain a visa to travel to the United States, DHS has implemented the Visa Security Program (VSP) through which U.S. Immigration and Customs Enforcement (ICE) deploys trained special agents overseas to high-risk visa activity posts. The VSP is currently deployed to 19 posts in 15 countries. As part of this program, ICE special agents conduct targeted, in-depth reviews of individual visa applications and applicants prior to the issuance of a visa and recommend to consular officers refusal or revocation of applications, when warranted. As of July 31, 2012, the VSP has screened over 1.1 million visa applicants against information held by DHS.

In support of ICE VSP efforts to enhance visa security measures, representatives from DHS, ICE, U.S. Customs and Border Protection (CBP) and DOS have agreed to develop an automated visa screening process that will enable DHS entities to identify derogatory information relating to applicants prior to the visa application being submitted to a Consular Officer. This process will inform and be used in conjunction with the current DOS Security Advisory Opinion (SAO) and Advisory Opinion (AO) programs. Additionally, DHS, DOS, and the intelligence community are working to establish a process to screen all visa applications against intelligence information provided by the interagency prior to visa issuance.

*Visa Waiver Program*

The VWP encourages high security standards and helps facilitate cooperation on security-related issues, including sharing security and law enforcement information, cooperating on repatriation matters, adhering to higher standards for aviation security, and strengthening document security standards. At the same time, the VWP facilitates exchanges—commercial, tourist, and others—that are essential to our economy. According to the Commerce Department, international tourism supported 1.2 million U.S. jobs last year, and tourism revenue in early 2012 was up 14% from the previous year. The VWP is an essential driver of international tourism because it allows eligible nationals of 36 countries to travel to the United States without a visa and remain in our country for up to 90 days. Over 60% of overseas travelers that come to the United States are from VWP countries.

DHS has focused on bringing VWP countries into compliance with the information sharing agreement requirements of *The Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act), Pub. L. No. 110–53. As of January 2012, all VWP countries have completed an exchange of diplomatic notes or an equivalent mechanism for the requirement to enter into an agreement to share information on lost and stolen passports with the United States through INTERPOL or other designated means. DHS, in collaboration with the Department of Justice (DOJ), has also concluded Preventing and Combating Serious Crime (PCSC) agreements, or their equivalent, with 35 VWP countries and two VWP aspirants. DHS, along with DOJ and DOS, continues to work closely with the remaining country to sign a PCSC agreement. These agreements enable each side to query the fingerprint databases of the other side for law enforcement purposes and enable the sharing of data about criminals and terrorists. Also, the U.S. Government has concluded negotiations on arrangements with all VWP countries for the exchange of terrorism screening information.

In addition, nationals from all VWP countries, regardless of their port of embarkation, are required to obtain an approved travel authorization via ESTA prior to boarding a carrier to travel by air or sea to the United States. ESTA vets prospective VWP travelers against several databases, including the terrorist watch list, lost and stolen passports (including INTERPOL Stolen and Lost Travel Documents), visa revocations, and previous VWP refusals.

DHS supports the carefully managed expansion of the VWP to countries that meet the statutory requirements, and are willing and able to enter into a close security relationship with the United States. To this end, we support current bi-partisan efforts by the Congress to expand VWP participation and to promote international

travel and tourism to the United States while maintaining our strong commitment to security. Additionally, as part of the President's recent Executive Order (13597), we are working with partner countries to meet existing requirements and prepare for further expansion of the VWP.

*Refugee Vetting*

DHS is committed to conducting rigorous checks in order to ensure that individuals admitted to the United States, including those through the refugee program, do not threaten our security. Refugees often lack, for legitimate reasons, valid documents that establish their identity. The Department has instituted rigorous methods to mitigate this vulnerability. In May 2007, DHS announced and implemented an administration-coordinated, enhanced background and security check process for Iraqi refugees applying for resettlement in the United States.

DHS has enhanced this security check regime, including both biographic and biometric checks, over the last several years as new opportunities and interagency partnerships with the law enforcement and intelligence communities have been identified. The latest enhancement to the refugee security check regime involves a new "pre-departure" check shortly before refugees are scheduled to travel to the United States. It is intended to identify whether any new derogatory information exists since the initial checks were conducted. No case is approved until results from all security checks have been received and analyzed.

SCREENING PRIOR TO BOARDING/DEPARTURE

The next layer of defense for air travel includes information-based and physical screening prior to a traveler boarding an aircraft. In partnership with the airline industry and foreign governments, the U.S. Government conducts passenger manifest screening and vetting prior to air travel to identify known threats. Passenger and crew manifest screening and vetting are also conducted for commercial vessels in the maritime environment. In addition, physical screening of all air passengers and their baggage is conducted at airport checkpoints.

The actions resulting from inclusion on the No-Fly, Selectee, or Expanded Selectee list are generally as follows:

- No-Fly matches are prohibited from boarding an aircraft;
- Selectee matches undergo enhanced screening prior to boarding an aircraft; and
- Expanded Selectee matches undergo enhanced screening prior to boarding an aircraft.

*Advance Passenger Information System (APIS) and Passenger Name Record (PNR) Data*

DHS use of APIS and PNR data has assisted CBP in the positive identification of over 4,000 persons with ties to terrorism in fiscal year 2011.

DHS analysis of PNR information—the information provided to the air carrier when booking international travel—is an indispensable tool for the prevention of terrorist travel. PNR analysis assists in the identification of watch-listed and other high-risk individuals up to 96 hours in the maritime environment and 72 hours in the air environment prior to departure.

DHS also uses PNR data to link previously unknown terrorists and criminals to known terrorists or criminals, and identify high-risk travelers by matching them against travel patterns known to have been used by terrorists or other intelligence-based scenarios.

DHS identifies travel patterns and other information to develop targeting rules from intelligence information. These rules are reviewed quarterly by CBP, the DHS Privacy Office, the DHS Office of Civil Rights and Civil Liberties (CRCL), and the Office of the General Counsel. Additionally, the DHS Chief Privacy Officer conducts privacy compliance reviews of the DHS use of PNR and reports the findings to Congress.

APIS data—essentially the flight or ship passenger and crew manifest for a given flight or voyage—contains information such as a traveler's date of birth, citizenship, and travel document number, which is typically collected as passengers check in for their flight or voyage.

*Pre-departure Screening*

DHS utilizes the Immigration Advisory Program (IAP), at 11 airports in nine countries, to conduct additional screening for high-risk and improperly documented travelers, by using targeting and passenger analysis information. At the invitation of foreign partners, IAP officers can make "no-board" recommendations to airlines for travelers who may present security risks or lack necessary travel documents. This partnership has also benefited air carriers, as it saves them time and the cost

of transporting individuals denied entry to the United States back to their port of embarkation. Through direct networks with commercial airlines and connections to CBP officers overseas as part of the IAP, National Targeting Center (NTC) officials are able to issue no-board recommendations to the airline to keep suspected high-risk passengers from traveling to the United States. In fiscal year 2012, to date, there have been more than 3,663 "no-board" recommendations.

*Maritime Environment*

As the lead DHS agency for maritime homeland security, the U.S. Coast Guard screens all commercial vessel passenger and crew manifests against intelligence holdings and law enforcement data sets. This screening is conducted through the vessel's submission of an Advanced Notice of Arrival (ANOA) up to 96 hours (but no less than 24 hours) prior to arrival at a U.S. port. In 2011, 28.5 million people and over 121,000 ship arrivals were screened, and 120 advance warning reports were generated regarding arriving ships, people, or cargo posing a potential threat.

*Checkpoint Screening*

DHS employs measures both seen and unseen by travelers, including walk-through metal detectors, explosive trace detection equipment, trained canines, vapor trace machines that detect liquid explosives, full-body pat-downs, and behavior detection officers—both at and beyond the checkpoint. Advanced Imaging Technology (AIT) machines are also employed to screen passengers for metallic and non-metallic threats that cannot be detected by walk-through metal detectors. DHS has also strengthened the presence and capacity of law enforcement to prevent terrorist attacks on commercial aviation.

DHS has increased Federal Air Marshal Service (FAMS) coverage of U.S.-flag carriers' international flights. The expanded FAMS program builds upon additional programs created since 9/11 that further increase the safety of aircraft, including the hardening of cockpit doors.

INSPECTION AT A PORT OF ENTRY

All travelers to the United States, regardless of the means by which they arrive (land, sea, or air), must present valid travel and identity documents in order to obtain admission. Upon arrival at a port of entry, a traveler presents his or her secure travel document (i.e., passport) and visa (if required) or other appropriate travel authorization. The CBP officer will conduct information-based checks against Federal databases, and, when applicable, will collect biometrics (including fingerprints) to vet them against the DHS Automated Biometric Identification System (IDENT). IDENT will match biometric data previously collected from the traveler, such as during the visa application or a past visit to the United States, to verify the person's identity. Travelers may also undergo a secondary inspection prior to an admissibility determination.

IDENT enables DHS to store and analyze biometric data—digital fingerprints and photographs—and then link that data with biographic information to establish and verify identities; IDENT contains biometric data on known and suspected terrorists, criminals, and immigration violators, and aids in distinguishing potential threats from bona fide travelers. "Anchoring" an identity on the first encounter—usually with the collection of biometrics through the visa and entry processes—helps prevent misidentifications and dramatically reduces the ability of individuals to use fraudulent identities on subsequent encounters.

*Western Hemisphere Travel Initiative*

DHS continues to balance the need to prevent terrorist travel with the need to facilitate the legitimate travel of known individuals. The Western Hemisphere Travel Initiative (WHTI), implemented for air travel in 2007 and travel by land and sea in 2009, requires all travelers—U.S. citizens and aliens alike—to present a passport or another acceptable secure document denoting identity and citizenship for entry into the United States. WHTI also expanded the use of radio frequency identification (RFID) technology to efficiently balance security needs and facilitation of legitimate trade and travel, resulting in an almost five-fold increase in RFID-enabled documents in 2 years. In addition to a decrease in counterfeit documents, and altered documents, WHTI has contributed to reduced wait times at ports of entry through Ready Lanes, which expedite the travel of individuals possessing WHTI-compliant and RFID-enabled documents.

*Global Entry*

In an effort to ensure security while facilitating legitimate trade and travel, DHS has also expanded Global Entry, which allows pre-approved, low-risk travelers expe-

dited inspection at select airports. More than 1 million trusted traveler program members are able to use the Global Entry kiosks, and we are expanding the program both domestically and internationally as part of the administration's efforts to foster increased travel and tourism.

In addition to U.S. citizens and Lawful Permanent Residents, Mexican nationals can now enroll in Global Entry, and Global Entry's benefits are also available to Dutch citizens enrolled in the Privium program; South Korean citizens enrolled in the Smart Entry Service program; Canadian citizens and residents through the NEXUS program; and citizens of the United Kingdom, Germany, and Qatar through limited pilot programs. In addition, we have signed agreements with Australia, New Zealand, Panama, and Israel to allow their qualifying citizens and permanent residents to participate in Global Entry. Global Entry applicants, like applicants for DHS's other Trusted Traveler programs (i.e., NEXUS, SENTRI, and FAST) are vetted against criminal and terrorist databases, and provide biometrics prior to acceptance into the program.

## SCREENING WITHIN THE UNITED STATES

Foreign visitors to the United States may undergo additional screening while in the United States for a variety of reasons, including if the visitor chooses additional domestic travel.

*Secure Flight*

In November 2010, DHS achieved a major aviation security milestone by assuming responsibility from the airlines for terrorist watch list screening for 100 percent of aircraft operators covered by the Secure Flight Final Rule for flights into, out of, and within the United States. This year, DHS expanded the program to include overflights (i.e., flights that pass over but do not land in the United States) by requiring all Foreign Air Carriers to report Secure Flight passenger data for covered flights. Transportation Security Administration (TSA) continues to work with foreign air carriers to ensure compliance of this requirement. In addition to facilitating secure travel for all passengers, Secure Flight helps prevent the misidentification of passengers who have names similar to individuals on Government data sets.

DHS revised the Secure Flight program to screen passengers against all records on the Terrorist Screening Database (TSDB) that contain a full name and a full date of birth (not just the No-Fly and Selectee lists); travelers identified under this new initiative are designated for enhanced physical screening prior to boarding an aircraft.

DHS uses a passenger's name, date of birth, and gender to vet airline passengers against terrorist information up to 72 hours before those passengers are permitted to board planes. Passengers who are potential matches are immediately identified by DHS for appropriate notifications and coordination with our Federal partners.

Secure Flight screens more than 14 million passenger reservations against terrorist information each week. Approximately 25 individuals per month are denied boarding under the Secure Flight program.

*TSA PreCheck™*

DHS has worked to develop a strategy for enhanced use of intelligence and other information to support a more risk-based approach in all facets of transportation security. TSA PreCheck™ is part of the Department's on-going effort to implement risk-based security concepts that enhance security by focusing on travelers DHS knows least about. More than 2 million passengers have received expedited screening through TSA PreCheck™ security lanes since the initiative began last fall. TSA PreCheck™ is now available in 22 airports for select U.S. citizens traveling domestically on Alaska Airlines, American Airlines, Delta Air Lines, United Airlines, and US Airways, and members of CBP's Trusted Traveler programs. TSA expanded TSA PreCheck™ benefits to U.S. military active-duty members traveling through Ronald Reagan Washington National and Seattle-Tacoma International airports. In addition to TSA PreCheck™, TSA has implemented other risk-based security measures including modified screening procedures for passengers 12 and younger and 75 and older.

As always, DHS will continue to incorporate random and unpredictable security measures throughout the security process, and at no point are TSA PreCheck™ travelers guaranteed expedited screening.

## SCREENING UPON DEPARTURE

Over the past year, we have worked to better detect and deter those who overstay their lawful period of admission. These efforts, and DHS's overall approach is documented extensively in the comprehensive biometric air exit plan submitted to Con-

gress this past spring. The ability to identify and sanction overstays is linked to our ability to determine who has arrived and departed from the United States. By matching arrival and departure records, and analyzing entry and exit records stored in our systems and using additional data collected by DHS, we can better determine who has overstayed their lawful period of admission.

In May 2011, DHS began a coordinated effort to vet all potential overstay records against intelligence community and DHS holdings for National security and public safety concerns. Using those parameters, we reviewed the backlog of 1.6 million overstay leads in the U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT) program and referred leads based on National security and public safety priorities to ICE for further investigation.

Through limited automated means, DHS cross-referenced additional overstay leads with DHS location and immigration holdings, closing additional records by confirming changes in immigration information or travel history that had not yet been recorded. Previously, these records would not have been examined, except in instances when resources allowed. Now, we are vetting all overstays for public safety and National security concerns, and DHS is also conducting automated reviews for changes in immigration status or travel history. This is performed on a recurrent basis.

In July, following the submission of the comprehensive air exit plan, Congress approved DHS to continue improvements related to identifying individuals who may have overstayed their lawful period of admission. DHS is implementing elements, and expects to have these enhancements in place by early 2013. Once completed, this initiative will significantly strengthen our existing capability to identify and target for enforcement action those who have overstayed their authorized period of admission, and who represent a public safety and/or National security threat by incorporating data contained within law enforcement, military, and intelligence repositories.

This strategy also will also enhance our ability to identify individual overstays; provide DOS with information to support visa revocation; prohibit future VWP travel for those who overstay; execute "lookouts" for individuals who overstay, in accordance with existing Federal laws; establish greater efficiencies to the VWP; and enhance the core components of an entry-exit and overstay program.

Concurrently, the Department's Science and Technology Directorate (S&T) is working to establish criteria and promote research for emerging technologies that would provide the ability to capture biometrics and develop a biometric exit capability at a significantly lower operational cost than is currently available. S&T is collaborating with the National Institute of Standards and Technology (NIST) on this initiative.

Last, as part of the Beyond the Border Action Plan signed by President Obama and Canadian Prime Minister Harper in December 2011, we are creating an exit program on the United States Northern Border. In accordance with the Action Plan, the United States and Canada will exchange entry records so that an entry to one country essentially becomes an exit record from the other country.

Overall, these elements constitute DHS's comprehensive approach to biometric exit implementation.

## BUILDING BRIDGES: INTERNATIONAL PARTNERSHIPS AND INFORMATION SHARING

DHS works closely with international partners, including foreign governments, major multilateral organizations, and global businesses, to strengthen the security of the networks of global trade and travel, upon which our Nation's economy and communities rely. Today, DHS is in just about every corner of the world, with 11 components and over 1,400 personnel stationed in more than 75 countries.

### *Perimeter Security*

DHS is working to implement the President's February 2011 Beyond the Border declaration with Canadian Prime Minister Harper, which will strengthen North American security and make both Canada and the United States safer through a series of mutually beneficial initiatives. Specifically, we have jointly committed to taking a "perimeter" approach to security and economic competitiveness in North America, and thus to collaborating to address threats well before they reach our shores. To address threats early, the United States and Canada are improving our intelligence and information sharing, and developing joint and parallel threat assessments in order to support informed risk-management decisions. We also are enhancing our efforts to identify and screen travelers at the earliest point possible, with a common approach, including biometrics. Specifically, we are working toward common technical standards for the collection, transmission, and matching of biometrics that enable the sharing of traveler information.

DHS and DOS have worked with our closest allies to develop routine sharing of biometric information collected for immigration purposes. Last year, DHS chaired an initiative with Australia, Canada, New Zealand, and the United Kingdom to build on these efforts and expand security and information-sharing cooperation to mutually enhance travel security among these five countries. A program that began in 2010, which shares biometric information with Australia, Canada, New Zealand, and the United Kingdom, has identified cases of routine immigration fraud, as well as dangerous people traveling under false identities.

*Intelligence and Information Sharing*

A critical step to thwarting terrorist operations along travel pathways is to identify those associated with, suspected of being engaged in, or supporting terrorist or other illicit activities, as well as the techniques they use to avoid detection. This is done by collecting, maintaining, and updating data and integrating knowledge of terrorist travel patterns into our immigration and border inspection systems and operations. DHS has created a standing intra-departmental working group to facilitate the sharing of DHS travel data with the intelligence community. The DHS Privacy Office and CRCL are key participants in the working group.

Since 9/11, the Federal Government has improved the sharing of information and intelligence among stakeholders. Several organizations within DHS provide critical resources to the Department's ability to understand, anticipate, and thwart terrorist travel.

CBP's National Targeting Center (NTC) provides tactical targeting information aimed at interdicting terrorists, criminal actors, and implements of terror or prohibited items. Crucial to the operation of the NTC is CBP's Automated Targeting System, a platform used by CBP to match travelers and goods against information and known patterns of illicit activity often generated from successful case work and intelligence. Since its inception after 9/11, the NTC has evolved into two Centers: The National Targeting Center Passenger (NTC–P) and the National Targeting Center Cargo (NTC–C).

DHS implements programs around the world to provide training and technical assistance to build the capacity of foreign governments to counter terrorism activity, prevent terrorist movement, and strengthen the security of the United States. It is imperative that officials have the proper training and access to intelligence to detect fraudulent travel documents so that such documents cannot be used by terrorists seeking to subvert the screening process. The ICE Forensic Document Laboratory (FDL) is the U.S. Government's only forensic crime laboratory dedicated exclusively to fraudulent document detection and deterrence. The FDL also provides training to international and domestic partners on identifying fraudulent documents.

REDRESS

With all of these efforts, DHS is deliberate in its effort to give travelers an opportunity to be heard when an issue arises. The Department has established the DHS Traveler Redress Inquiry Program (DHS TRIP), a single point of contact for individuals, regardless of citizenship, who have inquiries or seek resolution of difficulties they experience during travel, including: Denied or delayed airline boarding; denied or delayed entry into and/or exit from the United States; or frequent referral for additional screening. Individuals who complete the redress process are issued a redress number that can be used to book travel to prevent misidentifications.

PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES

Protecting privacy, civil rights, and civil liberties is a core mission of DHS. DHS has the first statutorily-required privacy office of any Federal agency, as well as a senior official responsible for civil rights and civil liberties. DHS builds privacy and civil rights and civil liberties protections into its operations, policies, programs, and technology deployments from the outset of their development.

Both the DHS Privacy Office and CRCL partner with every DHS component to assess policies, programs, systems, technologies, and rule-makings for privacy and civil liberties risks, and recommends appropriate protections and methods for handling personally identifiable information in accordance with the Constitution, the Privacy Act, and the Fair Information Practice Principles. At DHS we work hard to create an environment where privacy, civil rights, and civil liberties and security go hand-in-hand, helping to secure our Nation while honoring the principles on which the country was founded.

CONCLUSION

Since 9/11, we have learned that preventing terrorist travel through immigration and border security is more than drawing a line in the sand where we can deny entry into our country. We must utilize a multi-layered, many-faceted, and multi-national effort that weaves together intelligence, information-sharing, security and law enforcement programs from DHS, the interagency, and across a multitude of partnerships with our international and domestic partners.

Together they reflect one of our Nation's most pressing priorities: The facilitation of legitimate travel and commerce while thwarting threats, and simultaneously protecting privacy and civil liberties.

Thank you again for this opportunity to testify. I look forward to answering any questions you may have.

Mrs. MILLER. Thank you very much.

The Chairwoman now recognizes Mr. McAleenan. I hope I am pronouncing that correct.

**STATEMENT OF KEVIN MC ALEENAN, ACTING ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, CUSTOMS AND BORDER PROTECTION, DEPARTMENT OF HOMELAND SECURITY**

Mr. MCALEENAN. Very close, ma'am. McAleenan. Good morning. Chairwoman Miller, Ranking Member Cuellar, distinguished Members of the subcommittee, thank you for the opportunity to testify here this morning about U.S. Customs and Border Protection's efforts to disrupt terrorist travel.

On the 11th anniversary of the 9/11 terrorist attacks, CBP remains vigilant and focused. As the Nation's unified border security agency, CBP is responsible for securing our Nation's borders while facilitating legitimate trade and travel that is so vital to our economic health.

Within this broad responsibility, our priority mission is to prevent terrorists and terrorist weapons from entering the country. As a result of this committee's support, our strong Government and private-sector partnerships, advances in technologies and applications of intelligence, CBP and DHS are more capable than ever before in our efforts to identify and mitigate terrorist threats before they reach the United States.

A traveler's risk is now assessed from the moment he or she applies for a visa through the Department of State or for travel authorization through CBP's ESTA Program. To address the higher risk in the international air environment, which remains a primary target for terrorist organizations seeking to move operatives or attempt attacks, CBP leverages advanced travel information from air carrier reservation and check-in systems.

CBP's National Targeting Center, or NTC, analyzes this data through the automated targeting system, and uses advanced software to apply intelligence-driven targeting rules to conduct risk assessments. If information indicating a potential risk is discovered, NTC will issue a no-board recommendation to air carriers, preventing travel of a suspect individual.

Internationally, the NTC supports the work of CBP's Immigration Advisory Program to extend the Nation's zone of security beyond our physical borders to 11 airports in nine foreign countries, where we work with carriers and foreign authorities to identify and address potential threats prior to boarding.

To put our pre-departure efforts in context, in fiscal year 2009, before the Christmas day attempt, the NTC and IAP teams made fewer than 500 no-board recommendations to carriers for security purposes. This fiscal year, in contrast, the NTC and IAP teams have made almost 4,000 no-board recommendations, a dramatic increase that has have enhanced the security of our borders and international air travel.

While the focus of our pre-departure work is the air environment, we also maintain robust protocols upon arrival at U.S. ports of entry. Prior to admission at any U.S. port of entry, whether by air, land, or sea, CBP officers further assess traveler risk by scanning entry and identity documents, conducting personal interviews, and running appropriate biometric and biographic queries against law enforcement databases.

If there are any matches to suspected terrorist records, CBP activates its counter-terrorism response protocols. These protocols are aided by the fact that the National Targeting Center has become a critical interagency counter-terrorism resource, with representatives from over a dozen departments and agencies, including full units from ICE, TSA, the U.S. Coast Guard, and soon to be the Department of State.

Together we are assessing risk at each stage in the travel cycle and working together to enhance our collective response.

As this committee is well aware, we continue to live in a world of ever-changing threats. We must adapt and evolve to identify and address security gaps and anticipate vulnerabilities. CBP will continue to be at the forefront of the global effort against terrorism. We will work with our colleagues within DHS, Department of State, and the intelligence and law enforcement communities to meet these challenges.

Thank you again for the opportunity to testify about our work at CBP on this solemn anniversary. I look forward to answering your questions.

[The prepared statement of Mr. McAleenan follows:]

PREPARED STATEENT OF KEVIN MCALEENAN

SEPTEMBER 11, 2012

Good morning Chairman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee. Thank you for the opportunity to appear before you to represent U.S. Customs and Border Protection (CBP) and, on this solemn anniversary, to discuss our efforts to disrupt terrorist travel and promote travel security. I appreciate the committee's leadership and your continued efforts to ensure the security of the American people.

CBP'S ACTIONS TO PREVENT TERRORIST TRAVEL

As the unified border security agency of the United States, CBP is responsible for securing our Nation's borders while facilitating the flow of legitimate international travel and trade that is so vital to our Nation's economy. Within this broad responsibility, our priority mission remains to prevent terrorists and terrorist weapons from entering the United States.

To do this, CBP works in close partnership with the Federal counterterrorism community, including law enforcement agencies, the intelligence community, U.S. Immigration and Customs Enforcement (ICE), the Transportation Security Administration (TSA), the Department of State, State and local law enforcement, the private sector, and our foreign counterparts to improve our ability to identify risks as early as possible in the travel continuum, and to implement security protocols for addressing potential threats. CBP works with its counterparts to apply its capabilities at

multiple points in the travel cycle to increase security by receiving advance information, employing sophisticated targeting systems to detect risk, and acting through a global network to address risks or prevent the movement of identified threats toward the United States at the earliest possible point in their travel.

In concert with its partners, CBP strives to ensure that travelers who present a risk are appropriately interviewed or vetted before boarding a flight bound for the United States, and that any document deficiencies are addressed before traveling to the United States. CBP has placed officers in strategic airports overseas to work with carriers and host nation authorities, and has built strong liaisons with airline representatives to improve our ability to address threats as early as possible and effectively expand our security efforts beyond the physical borders of the United States.

These efforts seek to keep our transportation sectors safe and prevent threats from ever reaching the United States. These efforts also enhance efficiency and create savings for the U.S. Government and the private sector by preventing inadmissible travelers from traveling to the United States.

## TRAVEL TO THE UNITED STATES

Given that commercial air transportation remains the primary target of terrorist organizations seeking to attack the homeland or move operatives into the United States, my testimony will focus on international air travel. CBP inspects nearly 1 million travelers each day as they enter the United States, and about 30 percent—almost 100 million a year—of these travelers arrive via commercial aviation. CBP has developed and strategically deployed resources to detect, assess and, if necessary, mitigate the risk posed by travelers throughout the international travel continuum. CBP and its partners work to address risk at each stage in the process: (1) The time of application to travel; (2) ticket purchase or reservation; (3) check-in at a foreign airport; and (4) arrival in the United States. Aspects of this strategy are highlighted below.

### *Application to Travel*

In general, most non-U.S. citizens wishing to travel to the United States need to either apply for a visa from the Department of State (DOS) at a U.S. Embassy or Consulate, or a travel authorization from CBP via the Electronic System for Travel Authorization (ESTA). CBP plays an important role in each of these processes.

#### *Non-Immigrant Visa Process*

Travelers that require Non-Immigrant Visas (NIVs) to travel to the United States must apply to DOS to be a temporary visitor under specific visa categories, including those for business, pleasure, study, and employment-based purposes.

DOS manages the process of initially vetting visa applicants including biometric and biographic checks. DOS Consular Officers then adjudicate the visa application, which may include an interview of the applicant, to determine eligibility. Applicants suspected of committing fraud or suspected of other criminal or terrorist links are referred to DOS, or the appropriate agency, for additional investigation.

CBP operates and monitors the Visa Hot List, a tool to re-vet previously-issued visas against lookout records, to identify persons whose eligibility for a visa or entry to the United States has changed since the issuance of that visa. Relevant information that is uncovered is passed to DOS, ICE, or other agencies as appropriate. This continuous re-vetting by CBP has resulted in the revocation of over more than 3,000 visas by DOS since its inception in March 2010.

To further enhance visa screening efforts, ICE, CBP, and DOS are collaborating on the development of an automated visa application screening process that will broaden the scope to identify potential derogatory information prior to visa adjudication and issuance, and synchronize reviews of the information across these agencies. This process may be used as a precursor to and in conjunction with the current DOS Security Advisory Opinion (SAO) and Advisory Opinion (AO) programs. The joint program will leverage the three agencies' expertise, authorities, and technologies, such as CBP's Automated Targeting System (ATS), to screen pre-adjudicated visa applications. It will significantly enhance the U.S. Government's anti-terrorism efforts, improving the existing process by extending our borders outward and denying high-risk applicants the ability to travel to the United States.

*Electronic System for Travel Authorization (ESTA)*

Since 2009, travelers traveling to the United States by air or sea and intending to apply for admission under the Visa Waiver Program (VWP),[1] must first apply for travel authorization through CBP's on-line application system, the Electronic System for Travel Authorization (ESTA). Through this process, CBP incorporates targeting and database checks to identify those who are statutorily ineligible to enter the United States under the VWP and those who may pose a National security or criminal threat if allowed to travel. The majority of ESTA applications are approved; however, if derogatory information is revealed during the vetting process, the application is denied and the applicant is directed to DOS to initiate a formal visa application process. In fiscal year 2012 (through August 2012), CBP has vetted over 10.7 million ESTA applications and denied more than 21,000.

*Ticket Purchase/Reservation*

*Passenger Name Record*

As part of CBP's layered enforcement and risk segmentation approach, the next opportunity to review a traveler's information occurs upon the purchase of a ticket, when the carrier creates a Passenger Name Record (PNR). All commercial airlines are required to make their PNR systems and data available to CBP. The PNR is provided to CBP up to 72 hours in advance of travel, which permits CBP to conduct research and risk segmentation on all travelers including U.S. citizens and non-U.S. citizens. At this point, CBP, in cooperation with other Government agencies, begins a more comprehensive assessment of each traveler's risk by reviewing his/her travel documents, responses to questions on the ESTA or visa application, travel companions, and patterns of travel to identify those who may be ineligible to travel or who may warrant additional vetting.

*Check-in*

*Advance Passenger Information System*

Advance Passenger Information System (APIS) regulations require that carriers transmit all passenger and crew manifest information before departure, prior to securing the aircraft doors. APIS data includes the biographic traveler information that is found in a passport, such as a name and date of birth. APIS data also includes itinerary information, such as the date of travel and flight information. This information is used by CBP, in conjunction with the PNR data, to identify known or suspected threats before they depart the foreign location.

In 2007, CBP published the APIS Pre-Departure Final Rule, enabling CBP systems to conduct vetting prior to passengers gaining access to the aircraft or departing on-board a vessel. This regulation added an essential layer to our anti-terrorism security measures. As part of the implementation of the regulation, CBP developed an interactive communications functionality where carriers can transmit single-passenger APIS messages as passengers check-in and receive an automated response message.

As part of the Department of Homeland Security (DHS) commitment to establish a common reporting process for carriers submitting traveler information to DHS components, CBP and TSA aligned the CBP APIS Pre-Departure requirements with those of the TSA Secure Flight program, so that air carriers transmit data once and receive a combined DHS response message that includes both the TSA Secure Flight screening results and the traveler's ESTA status. This consolidated information helps carriers make informed boarding decisions. CBP is currently expanding this capability to include a document validation check, to provide confirmation to the airlines that the individual's visa is valid as well.

*National Targeting Center*

CBP leverages all available advance passenger data including the PNR and APIS data, previous crossing information, intelligence, and law enforcement information, as well as open-source information in its anti-terrorism efforts at the National Targeting Center (NTC). The NTC is a 24/7 operation that makes extensive use of intelligence materials and law enforcement data, allowing analysts and targeting officers to make tactical decisions at all points along the travel continuum. Starting with the earliest indications of potential travel, including United States-bound travel res-

[1] The 36 countries currently designated for participation in the Visa Waiver Program include: Andorra, Australia, Austria, Belgium, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, South Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

ervations, ESTA applications, visa applications, and passenger manifests, and continuing through the inspection or arrivals process, the NTC is continually analyzing information gleaned from these sources using CBP's Automated Targeting System (ATS). ATS is a decision-support tool for CBP officers which compares information on travelers arriving in, transiting through, and exiting the country against law enforcement and intelligence databases to identify individuals requiring additional scrutiny. This information is also matched against targeting rules developed by subject matter experts. Targeting rules are based on actionable intelligence derived from current intelligence community reporting or other law enforcement information available to CBP.

NTC analyzes each traveler's risk before departure to identify possible matches to the U.S. Government's consolidated terrorist watch list, Interpol lost and stolen passports, criminal activity, fraud, and other mala fide travelers, including U.S. citizens. Through direct networks with commercial airlines and connections to CBP officers overseas as part of the Immigration Advisory Program (IAP), NTC officials are able to issue no-board recommendations to the airline to keep suspected high-risk passengers from traveling to the United States. In fiscal year 2011, NTC made 3,181 no-board recommendations to carriers. In fiscal year 2012 (through August 2012), there have been more than 3,600 no-board recommendations. The NTC vetting process for international passengers continues while the flight is en route to the United States in order to identify any travelers who, although they may not be National security risks, may need to be referred for a more thorough inspection at the first port of entry upon arrival in the United States for other potential violations.

In addition to expanding the Nation's zone of security beyond the United States and improving operational efficiency, NTC pre-departure programs result in significant monetary savings by preventing inadmissible passengers from boarding flights destined to the United States, where upon arrival most of them likely would have to be processed by CBP for refusal or removal, generating detention costs for the U.S. Government and additional repatriation expenses for commercial carriers.

In a recent effort to make CBP passenger and cargo targeting more effective, the NTC was established as a stand-alone entity in the Office of Field Operations with greater responsibility for CBP passenger and cargo targeting operations at the port of entry. The NTC continues to improve its operations as DHS and CBP anti-terrorism targeting requirements expand by exploring new and innovative ways to identify, interdict, or deter terrorists, their weapons, and their supporters.

*Immigration Advisory Program*

IAP is another integral component of CBP's layered security approach. With advance targeting support from the NTC, IAP officers work in partnership with foreign law enforcement officials, to identify and prevent terrorists and other high-risk passengers, and then work in coordination with commercial air carriers to prevent these individuals from boarding flights destined to the United States. Maximizing the use of new mobile technology to enhance on-site targeting, IAP officers conduct passenger interviews and assessments to evaluate the potential risks presented by non-watchlisted travelers. The IAP is currently operational at 11 airports in 9 countries including Amsterdam, Doha, Frankfurt, London Heathrow and Gatwick, Madrid, Manchester, Mexico City, Panama City, Tokyo, and Paris.

Since the inception of the program in 2004, IAP officers have been successful in preventing the boarding of more than 15,700 high-risk and improperly documented passengers, to include matches to the TSDB.

*Arrival at a U.S. Port of Entry*

*Arrival Processing*

Upon arrival in the United States, all persons are subject to inspection by CBP officers. Upon application for admission to the United States, this inspection begins with CBP officers scanning the traveler's entry document and performing a query of various CBP databases for exact or possible matches to existing lookouts, including those of other law enforcement agencies. The system queries the document information against the APIS manifest information previously received from the carrier and provides any enforcement information about the traveler to the officer for appropriate action. APIS data is verified for completeness and accuracy through this process.

For most foreign nationals arriving at U.S. airports, fingerprint biometrics and photographs are captured by CBP officers. If the traveler has been previously fingerprinted, either at time of visa application or during a previous trip to the United States, the newly captured fingerprints will be compared to the originals to ensure the fingerprints match. Once a verified identity is established, the system

will identify any watch list information and return the results to the officer for appropriate processing. If the traveler has not been previously fingerprinted, the officer will collect all ten fingerprints and a biometric watch list search will be conducted, returning the search results to the officer. In addition to the biographic and biometric system queries performed, each traveler is interviewed by a CBP officer to determine the purpose and intent of their travel, and whether any further inspection is necessary based on concerns for National security, identity or admissibility, customs, or agriculture.

If upon review of the system queries there are any exact or possible matches to the TSDB, including potential matches to the "No-Fly" List, or other law enforcement lookouts, the NTC will be notified and coordinate with the port of entry for appropriate disposition or action. Additionally, CBP has established a Counter-Terrorism Response (CTR) protocol at ports of entry for passengers arriving with possible links to terrorism. CTR protocol mandates immediate NTC notification, initiating coordination with the Terrorist Screening Center (TSC), the National Counter Terrorism Center (NCTC), ICE, and the Federal Bureau of Investigation (FBI) Terrorist Screening Operations Unit (TSOU), and National Joint Terrorism Task Force (NJTTF).

For CBP's Preclearance locations in Aruba, Bermuda, the Bahamas, Canada, and Ireland, customs, agriculture, and immigration inspection and examination typically occurs at the Preclearance location instead of upon arrival in the United States. Therefore, this process allows the aircraft to arrive at a domestic airport gate in the United States and travelers may proceed to their final destination without further CBP processing; however, CBP may conduct further inspection or engage in enforcement action after a pre-cleared flight departing from a preclearance location arrives in the United States.

For CBP land border locations, the Western Hemisphere Travel Initiative (WHTI) implemented the first 9/11 Commission border security recommendation and legislative mandate by reducing the number of acceptable travel documents from more than 8,000 to a core set of six secure documents types which can be automatically queried via law enforcement databases as the vehicle approaches the CBP officer. Today, more than 16 million individuals have obtained Radio Frequency Identification (RFID) technology-enabled secure travel documents, which can be verified electronically in real-time back to the issuing authority, to establish identity and citizenship. The implementation of WHTI in the land border environment, and the increased use of RFID-enabled secure travel documents, have allowed CBP to increase the National law enforcement query rate, including the terrorist watch list, to over 98 percent. By comparison, in 2005, CBP performed law enforcement queries in the land border environment for only 5 percent of travelers.

As of June 2009, all major land border ports, representing 95 percent of all inbound vehicle traffic, have been upgraded to include improved license plate readers, RFID readers, and improved processing applications to facilitate the inspection of travelers and vehicles using the new RFID-enabled travel documents. Since June 2009, the average number of imposter apprehensions, counterfeit and altered documents seized has declined to 42 per day from 84 per day (a 50 percent decrease).

*Outbound: Air, Land, and Sea*

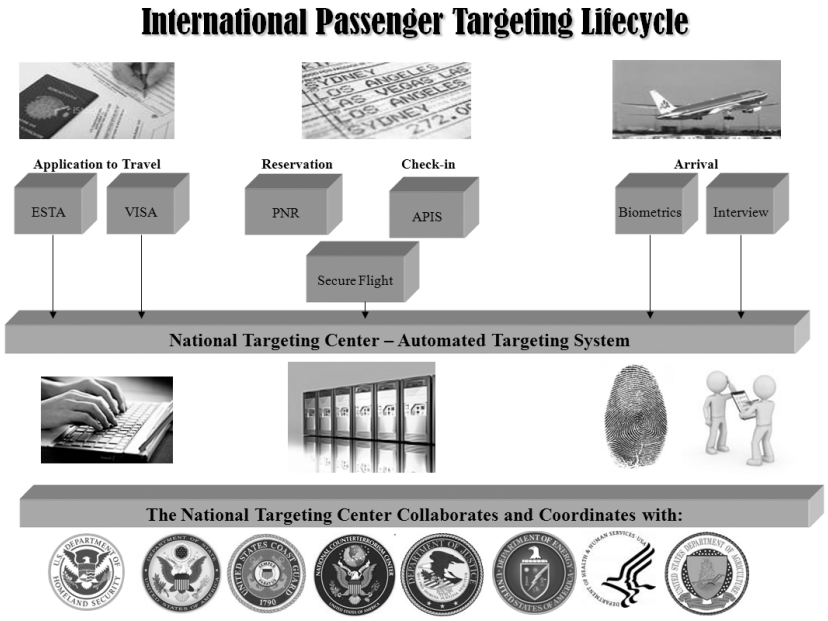
In addition to vetting inbound flights for high-risk travelers, CBP also developed protocols to enhance outbound targeting efforts within ATS, with the goal of identifying travelers who warrant outbound inspection or apprehension. Outbound targeting programs identify potential matches to the TSDB, including potential matches to the "No-Fly" List, as well as National Criminal Information Center fugitives, and subjects of active currency, narcotics, and weapons investigations. Additionally, outbound operations are enhanced by the implementation of targeting rules designed to identify and interdict subjects with a possible nexus to terrorism or links to previously identified terrorist suspects. As with inbound targeting rules, outbound targeting rules are continually adjusted to identify and interdict subjects of interest based on current threat streams and intelligence. Advance outbound manifest information is also obtained through the APIS system from carriers for all passengers 30 minutes prior to departure or if using the APIS Quick Query mode, then carriers can transmit in real time as each passenger checks in for the flight prior to boarding.

As soon as APIS information becomes available, prior to the departure of a commercial conveyance, CBP and the TSA immediately begin the screening and vetting processes of the outbound flight for possible inclusion in the TSDB, including potential matches to the "No-Fly" and Selectee List, as well as other law enforcement lookouts, using any and all available biographic information of the traveler. CBP's law enforcement capability and commitment to National security, through the moni-

toring and vetting of outbound flights, were highlighted on May 1, 2010 when CBP officers arrested Faisal Shazad as the man suspected in the Times Square car bomb plot as he attempted to flee the country on a flight destined to Dubai. Shazad had, hours before, come to the attention of Federal law enforcement authorities in part because of data collected by CBP. Later, when Shazad tried to flee the country by purchasing a ticket on his way to the airport, it was CBP's collection of API data that alerted us to his presence on the flight for Dubai, enabling us to take him into custody before the plane departed. CBP's capabilities were also evident in September 2009 when Najibullah Zazi plotted an attack against the New York City subway system; in this case, CBP's databases led to the identification of two of Zazi's previously unknown co-conspirators. One pled guilty in April 2010 and the other was found guilty on May 21, 2012. Also, in October 2009, David Coleman Headley was arrested and pled guilty to plotting attacks in Copenhagen and conducting surveillance in support of the November 2008 attacks in Mumbai, India; CBP identified Headley using partial name and travel routing provided by FBI.

CONCLUSION

CBP is committed to protecting our country from terrorists and terrorist weapons while ensuring safe international travel and facilitating legitimate trade. CBP is continually updating and adjusting our programs to enhance the overall efficiency of how we operate in this ever-changing global environment. As part of our mission, CBP fosters partnerships and encourages cooperation with the law enforcement community, industry, and foreign governments. CBP has built a multi-layered approach for screening and identifying potential travelers to the United States who may pose a threat to the homeland and will continue to use all means within our authority to protect the Nation and its citizens. Thank you for allowing me the opportunity to testify before you today, and I look forward to answering your questions.




Mrs. MILLER. Thank you very much.

The Chairwoman now recognizes Mr. Woods for his testimony.

**STATEMENT OF JOHN P. WOODS, ASSISTANT DIRECTOR, NATIONAL SECURITY INVESTIGATIONS, HOMELAND SECURITY INVESTIGATIONS, IMMIGRATIONS AND CUSTOMS ENFORCEMENT, DEPARTMENT OF HOMELAND SECURITY**

Mr. WOODS. Thank you, Chairwoman Miller. Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee, thank you for the opportunity to discuss ICE's efforts to prevent terrorist travel and the exploitation of our immigration system.

Visa overstays and other forms of status violation bring together two critical areas of ICE's mission, both National security and immigration enforcement. The importance of determining who to allow to enter the United States and ensuring compliance with conditions of such entry cannot be overstated.

As you know, ICE's Visa Security Program, or VSP, interdicts criminals, terrorists, and others who would exploit our legal visa process to enter the United States and serves as the agency's front line in protecting the United States against terrorist and criminal organizations.

The VSP integrates DHS, law enforcement equities into the visa process to advance our Nation's border security initiatives. Under the VSP, ICE special agents are assigned to visa security units at high-priority diplomatic posts world-wide to conduct visa security activities and help identify potential criminal and terrorist threats before they would have the opportunity to reach our ports of entry.

The VSP currently screens and vets selected non-immigrant and immigrant visa applications prior to visa issuance. In support of our efforts to enhance visa security measures, representatives on the panel here today from ICE, CBP, Department of State, including the U.S. intelligence community, are developing an automated visa screening process that will enable ICE to identify derogatory information related to all non-immigrant visa applicants prior to their adjudication by consular offices.

This process may be used as a precursor to or in conjunction with our current Department of State Security Advisory Opinion and Advisory Opinion Programs. When an alien files for non-immigrant visa application electronically, it goes to the Department of State's Consular Electronic Application Center, or the CEAC.

ICE's information technology modernization efforts will allow ICE to obtain the non-immigrant visa application information directly from CEAC, screen it against DHS and intelligence community data before it goes to consular offices for adjudication. This automated screening process will significantly enhance the U.S. Government's anti-terrorism efforts by aiding another layer of security to our border protection efforts.

In addition to VSP, ICE's Counter-Terrorism and Criminal Exploitation Unit, or the CTCEU, is dedicated to the enforcement of non-immigrant visa violation. Today through the CTCEU, ICE proactively develops cases for investigation through the Student Exchange Visitor Program and the US–VISIT Program.

These programs enable ICE to access information about millions of students, tourists, and temporary workers present in the United States at any given time, and identify those who have overstayed or otherwise violated the terms of their condition of admission.

Special agents and analysts at ICE monitor the latest threat reports and proactively address emergent issues. This practice has contributed to ICE's counter-terrorism mission by supporting high-priority National security initiatives based on specific intelligence.

The practice is designed to identify individuals exhibiting specific respecters risk factors on intelligence reporting, including international travel from specific geographic locations and in-depth research of dynamic social networks. This person-centric approach of non-immigrant prioritization moves away from our traditional methods of identification and thereby enhances the way threats are identified and resolved.

As we move forward, it is imperative that we continue to expand the Nation's enforcement efforts concerning overstays and other status violations, with special emphasis on those who threaten our National security and public safety. Accordingly, ICE is analyzing various approaches to this issue, including sharpening the focus of programs that address vulnerabilities that are exploited by visa violators, such as the DHS Overstay Initiative and CTCEU's School Fraud Targeting Program.

Effective border security measures require broad information sharing and cooperation among U.S. agencies. On January 11, 2011, ICE signed a memorandum of understanding outlining the roles and responsibilities and collaboration between ICE and the Department of State's Consular Affairs and Diplomatic Security.

This MOU governs the day-to-day operations of ICE agents conducting visa security operations at U.S. embassies and consulates abroad. To facilitate this information sharing, it reduces duplication of efforts by both ICE and the Department of State by supporting collaborative training and orientation prior to overseas assignments.

The VSP at high-priority U.S. embassies and consulates brings an important law enforcement element to the visa review process. This relationship serves as an avenue for VSP personnel to alert consular offices and other U.S. Government personnel to potential security risks.

More than a decade after the 9/11 attacks, ICE has made significant progress in preventing terrorists from exploiting our visa process. We look forward to working closely with the subcommittee in the future to enhance those efforts.

I want to thank you again for the opportunity to appear today. I would be pleased to answer any questions you have.

[The prepared statement of Mr. Woods follows:]

PREPARED STATEMENT OF JOHN P. WOODS

SEPTEMBER 11, 2012

INTRODUCTION

Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee: Thank you for the opportunity to discuss the efforts of U.S. Immigration and Customs Enforcement (ICE) to prevent terrorist travel and the exploitation of our immigration system. Visa overstays and other forms of status violation bring together two critical areas of ICE's mission—National security and immigration enforcement—and the importance of determining whom to allow to enter the United States and ensuring compliance with the conditions of such entry cannot be overstated.

THE VISA SECURITY PROGRAM (VSP)

The Visa Security Program (VSP) interdicts criminals, terrorists, and others who would exploit the legal visa process to enter the United States and serves as ICE's front line in protecting the United States against terrorist and criminal organizations. The VSP integrates DHS law enforcement equities into the visa process to advance the Nation's border security initiatives. Under VSP, ICE agents are assigned to Visa Security Units (VSU) at high-priority diplomatic posts worldwide to conduct visa security activities and help identify potential criminal and/or terrorist threats before they reach a United States port of entry.

The ICE VSP currently screens and vets selected non-immigrant and immigrant visa applications prior to visa issuance. In support of ICE VSP efforts to enhance visa security measures, representatives from DHS, ICE, U.S. Customs and Border Protection (CBP), the U.S. Department of State (DOS), and the U.S. intelligence community are developing an automated visa screening process that will enable DHS entities to identify derogatory information relating to all non-immigrant visa applicants prior to adjudication of their visa application by DOS consular officers. This process may be used as a precursor to, and in conjunction with, the current DOS Security Advisory Opinion and Advisory Opinion programs.

When an alien files a non-immigrant visa application electronically, it goes to the DOS Consular Electronic Application Center (CEAC) and is transmitted to DHS for screening against CBP and other DHS and intelligence community data. Through the automated visa screening process, currently under development, the information identified through this process will provide DOS consular officers information they can use in their interviews to address concerns raised by the VSP findings, adding another layer of security to our border protection efforts, in turn denying mala fide travelers access to the United States.

For the automated visa screening process under development, a proposed coordinated review process will be conducted by ICE and CBP. This process will include the capability to utilize CBP vetting methodologies, to address specific threats identified by the intelligence community, to provide detailed case notes and justifications for any recommendations for consular officers related to visa issuance, and to recommend applicants for targeted interviews, and incorporate feedback from DOS consular officers. DHS will work cooperatively with DOS to refine the review process to ensure the information provided is relevant, supported by immigration law, and efficient. A future expansion of this system will incorporate pre-adjudicative screening and vetting of immigrant visa applications.

Additionally, ICE has deployed Homeland Security Investigations (HSI) special agents assigned to the VSP to the National Targeting Center (NTC) and the National Counterterrorism Center (NCTC) to augment and expand current operations. The NTC provides tactical targeting and analytical research in support of preventing terrorists and terrorist weapons from entering the United States. The colocation of HSI special agents at the NTC and NCTC have helped to increase both communication and information sharing.

THE STUDENT AND EXCHANGE VISITOR PROGRAM (SEVP)

The Student and Exchange Visitor Program (SEVP) is a part of the National Security Investigations Division and facilitates information sharing among relevant Government partners on nonimmigrants whose primary reason for coming to the United States is to be students. On behalf of DHS, SEVP covers schools, nonimmigrant students in the F and M visa classifications and their dependents. The Student Exchange Visitor Information System (SEVIS) is the database that SEVP manages that monitors schools that have been certified by DHS to enroll foreign students, and the exchange visitor programs designated by the DOS to sponsor exchange visitors. SEVIS contains the records of more than 1.1 million active nonimmigrant students, exchange visitors, and their dependents, as well as nearly 10,000 SEVP-certified institutions.

SEVP regulates schools' eligibility to enroll foreign individuals for academic and vocational training purposes and manages the participation of SEVP-certified schools in the student and exchange visitor program, and nonimmigrant students in the F (academic) and M (vocational) visa classifications and their dependents. DOS manages the Exchange Visitor Program for nonimmigrants in the J (exchange visitor) visa classification.

SEVP is responsible both for certifying schools and for withdrawing certification from non-compliant schools. The certification process assists in the important functions of furthering National security and the integrity of our Nation's borders, by providing consistent, comprehensive oversight while preserving the rich tradition of welcoming nonimmigrant students and exchange visitors.

SEVP collects, maintains, and provides information to interagency partners so that only legitimate foreign students and exchange visitors gain entry to, and remain in, the United States. The result is an easily accessible system that provides timely information to support ICE's law enforcement mission, as well as to our DHS partner agencies, CBP and U.S. Citizenship and Immigration Services, and other Federal agencies. Additionally, the data maintained by SEVP in SEVIS support the DOS's Bureau of Consular Affairs visa process by providing advanced electronic data on nonimmigrant visa applicants prior to visa issuance.

The student and exchange visitor programs that bring F, J, and M visa holders to the United States are of immense value to all countries involved, as they serve to strengthen international relations and foster intercultural understanding. These programs produce economic benefits as well; the U.S. Department of Commerce estimates that foreign students and exchange visitors contributed more than $21 billion to the U.S. economy through their expenditures on tuition and living expenses during the 2010–2011 academic year.

THE COUNTERTERRORISM AND CRIMINAL EXPLOITATION UNIT (CTCEU)

Created in 2003, the Counterterrorism and Criminal Exploitation Unit is ICE's National program dedicated to the enforcement of nonimmigrant visa violations. Today, through the CTCEU, ICE proactively develops cases for investigation in cooperation with the SEVP and the United States Visitor and Immigrant Status Indicator Technology (US–VISIT) Program. These programs enable ICE to access information about the millions of students, tourists, and temporary workers present in the United States at any given time, and identify those who have overstayed or otherwise violated the terms and conditions of their admission.

Each year, the CTCEU analyzes records on hundreds of thousands of potential status violators from SEVIS and US–VISIT, along with other information. These records are reviewed for potential violations that would warrant field investigations, such as establishing compliance or confirming departure from the United States, or determining if additional derogatory information is available for analysis. Between 15,000 and 20,000 of these records are resolved by in-house analysts each month. Since its creation, analysts have resolved more than 2 million such records using automated and manual review techniques. On average, ICE opens approximately 6,000 investigative cases annually, and assigns them to our special agents in the field for further investigation.

Agents and analysts in ICE monitor the latest threat reports and proactively address emergent issues. This practice has contributed to ICE's counterterrorism mission by supporting high-priority National security initiatives based upon specific intelligence. The practice is designed to identify individuals exhibiting specific risk factors based on intelligence reporting, including international travel from specific geographic locations to the United States, and in-depth criminal research and analysis of dynamic social networks. This person-centric approach to nonimmigrant prioritization moves away from the traditional methods of identification, thereby enhancing the way threats are identified and resolved.

In order to ensure that the potential violators who pose the greatest threats to National security are given priority attention, ICE uses intelligence-based criteria, developed in close consultation with the intelligence and law enforcement communities. ICE assembles the Compliance Enforcement Advisory Panel (CEAP) on a triannual basis to ensure that it uses the latest threat intelligence to target nonimmigrant overstays and status violators who pose the greatest threats to National security and to discuss possible changes based on current threat trends. The CEAP is composed of members from the Federal Bureau of Investigation (FBI), the NCTC, DHS Office of Intelligence and Analysis, and other intelligence community members.

An ICE investigation in Los Angeles, California exemplifies how the CTCEU operates. In March 2011, the CTCEU received an INTERPOL blue notice concerning a person who traveled to the United States as a tourist. A blue notice seeks information (e.g., identity, criminal record) on subjects who have committed criminal offenses, and is used to trace and locate a subject where extradition may be sought (i.e., offenders, witnesses). The individual at issue in the Los Angeles investigation had an arrest warrant in connection with child pornography charges in Colombia. A week later, ICE special agents arrested the person who was admitted as a visitor and violated the terms of admission by working in the adult film industry.

Likewise, in March 2010, ICE's Counterterrorism and Criminal Exploitation Group in Miami, Florida, initiated "Operation Class Dismissed," a criminal investigation that led to the indictment of the owner/operator of a Miami-based foreign language school and one of its employees on four counts of conspiring to commit a

criminal offense against the United States. The owner and employee were suspected of fraudulently sponsoring foreign students by certifying students as nonimmigrants, without requiring them to maintain full courses of study to comply with the terms of their admission. ICE's primary focus in these types of investigations is the criminal violations of the business owner/operators and administrative violations of the students. This ICE investigation revealed that only approximately 5 percent of the school's students attended class on any given day. In addition to the indictment, follow-up investigation resulted in the administrative arrests of 116 student visa violators purported to be attending the school from multiple countries.

The CTCEU tracks 75 active criminal investigations each year. Since June 2010, HSI special agents have criminally arrested 39 school owners or officials related to fraud or and misuse of student visas. Additionally, 10 foreign nationals residing outside of the United States have been arrested for various student visa fraud schemes. During fiscal year 2012, HSI special agents have conducted 760 school outreaches Nation-wide, which represents a 400 percent increase over the previous fiscal year. CTCEU has reviewed 476 schools for fraud or National security anomalies that have resulted in 11 criminal investigations. All of this is being completed in concert with SEVP's on-going efforts to effectively build our Nation's population of well-qualified international students to a number that is as robust as that of pre-9/11. SEVP continues to work to close vulnerabilities within the program.

As we move forward, it is imperative that we continue to expand the Nation's enforcement efforts concerning overstays and other status violations with special emphasis on those who threaten National security or public safety. Accordingly, ICE is analyzing various approaches to this issue, including sharpening the focus of programs that address vulnerabilities exploited by visa violators, such as the DHS Overstay Initiative and school fraud targeting by CTCEU.

COORDINATION WITH US–VISIT AND OTHER DHS COMPONENTS

CTCEU also works in close collaboration with US–VISIT, part of the DHS's National Protection and Programs Directorate. US–VISIT supports DHS's mission to protect our Nation by providing biometric identification services to Federal, State, and local Government decision makers to help them accurately identify the people they encounter, and determine whether those people pose risks to the United States. DHS's use of biometrics under the US–VISIT program is a powerful tool in preventing identity fraud and ensuring that DHS is able to rapidly identify criminals and immigration violators who try to cross our borders or apply for immigration benefits under an assumed name. Interoperability between the FBI Criminal Justice Information Service's IAFIS and US–VISIT's Automated Biometric Identification System (IDENT), which includes the sharing of biometric information, is the foundation of ICE's Secure Communities program.

US–VISIT also analyzes biographical entry and exit records stored in its Arrival and Departure Information System to further support DHS's ability to identify international travelers who have remained in the United States beyond their periods of admission by analyzing related biographical information.

ICE receives or coordinates nonimmigrant overstay and status violation referrals from US–VISIT's Data Integrity Group from several unique sources: Overstay violations; biometric watch list notifications; CTCEU Visa Waiver Enforcement Program nominations; and enhanced biometric exit. The first type, nonimmigrant overstay leads, is used by the CTCEU to generate field investigations by identifying foreign visitors who violate the terms of their admission by remaining in the United States past the date of their required departure.

HSI generates a second type of lead from biometric data collected by US–VISIT. US–VISIT routinely receives fingerprint records from a variety of Government sources and adds them to a biometric watch list, including individuals of National security concern. These new watch list records are checked against all fingerprints in IDENT to determine if DHS has previously encountered the individual. If US–VISIT identifies a prior encounter, such as admission to the United States, the information is forwarded to ICE for review and possible field assignment. Similarly, US–VISIT monitors records for individuals who, at the time of admission to the United States, were the subject of watch list records that did not render the individuals inadmissible to the United States. Therefore, if such individuals overstay their terms of admission, information on the subjects is forwarded to ICE for review and possible referral to investigative field offices for follow-up.

The third type of lead pertains to the CTCEU's Visa Waiver Enforcement Program (VWEP). The Visa Waiver Program (VWP) is the primary source of nonimmigrant visitors from countries other than Canada and Mexico. Although the overstay rate from this population is less than 1 percent, ICE created a program

dedicated to addressing overstays from VWP. Prior to the implementation of the VWEP in 2008, there was no National program dedicated to addressing VWP. CTCEU provides US–VISIT a list of potential VWP overstays for additional scrutiny. In accord with its intelligence-based criteria, the relevant portion of this list is given to CTCEU's lead tracking system for review and possible field assignment.

Additionally, the CTCEU develops potential overstay and status violation leads from SEVIS and other sources, and applies intelligence-based criteria to determine whether an investigative referral is appropriate. Throughout its history, the integrity of SEVIS data and its applicability have been valued throughout the law enforcement community.

In May 2011, at the direction of Secretary Napolitano, DHS's Counterterrorism Coordinator organized an effort to ensure that all overstays, regardless of priority, receive enhanced National security and public safety vetting by the NCTC and CBP. As part of Phase 1 of this effort, DHS components reviewed a backlog of 1.6 million un-vetted potential overstay records based on National security and public safety priorities.

As of 2010, DHS had a backlog of "un-reviewed overstays," comprised of system-identified overstay leads, which did not meet criteria set by ICE for expedited high-priority review. Before the summer of 2011, these records would not have been examined, except in instances when resources allowed it. The DHS "overstay initiative," begun in the summer of 2011 at the direction of the Secretary, reformed this effort.

By leveraging capabilities within CBP's Automated Targeting System, as well as DHS's relationship with NCTC, DHS was able to conduct richer, more thorough vetting for National security and public safety concerns. This generated new leads for ICE, which previously would not have been uncovered.

### COORDINATION WITH DOS

Effective border security requires broad information sharing and cooperation among U.S. agencies. On January 11, 2011, ICE signed a memorandum of understanding (MOU) outlining roles, responsibilities, and collaboration between ICE and the DOS Bureaus of Consular Affairs and Diplomatic Security. The MOU governs the day-to-day operations of ICE agents conducting visa security operations at U.S. embassies and consulates abroad. To facilitate information sharing and reduce duplication of efforts, ICE and DOS support collaborative training and orientation prior to overseas deployments. Once they are deployed to overseas posts, ICE and DOS personnel work closely together in: Participating in working groups; coordinating meetings, training, and briefings; and engaging in regular and timely information sharing.

The VSP's presence at high-priority U.S. embassies and consulates brings an important law enforcement element to the visa review process. Additionally, this relationship serves as an avenue for VSP personnel to alert Consular Officers and other U.S. Government personnel to potential security threats in the visa process.

ICE continues to evaluate the need to screen and investigate additional visa applicants at high-risk visa issuing posts other than the 19 posts at which the agency currently operates, which were determined in collaboration between ICE and DOS. ICE will continue to conduct joint site visits with DOS to identify locations for deployment based on emerging threats. We are engaged with our counterparts at DOS in determining a common strategic approach to the broader question of how best to collectively secure the visa issuance process. We look forward to continuing to report back to you with updates on this process.

### RECENT SUCCESSES WITH OUR PARTNERS

Working in tandem with other DHS personnel, as well as our international, Federal, State, local, and Tribal partners, we have enjoyed significant successes preventing visa fraud. I would like to elaborate briefly on two of these cases.

In December 2010, ICE special agents were involved in the identification and investigation of a transnational alien smuggling organization that facilitated the illegal travel of Somali nationals into Yemen and on to western locations, including the United States. ICE special agents received information from the ICE Attaché office in Amman, Jordan that two Somali nationals had been intercepted in Amman attempting to travel to Chicago using counterfeit travel documents, and contacted local officials in Yemen and Somalia to investigate how the counterfeit documents had been obtained and how the subjects had transited Yemen. The information developed was shared with other U.S. agencies at post in Sana'a via the Law Enforcement Working Group, as well as ICE domestic offices and the appropriate FBI Joint

Terrorism Task Force. While the joint investigation is on-going, efforts to date have eliminated this scheme as a method of entry to the United States.

In May 2011, ICE special agents within the VSP Security Advisory Opinion Unit (SAOU) investigated a Middle Eastern national who obtained a nonimmigrant visa to enter the United States by concealing his true identity from DOS by using a variation of his true name. Through vetting efforts, the SAOU identified this individual's true identity and revealed that he was a known terrorist with significant ties to other known terrorists, and who was likely involved in the planning of a terrorist attack in 2003. Based on this investigation and at the request of the VSP and SAOU, DOS revoked the individual's visa on National security-related grounds and prevented him from traveling to the United States.

CONCLUSION

More than a decade after the attacks of 9/11, ICE has made significant progress in preventing terrorists from exploiting the visa process. Thank you again for the opportunity to testify today and for your continued support of ICE and its law enforcement mission.

I would be pleased to answer any questions you may have.

Mrs. MILLER. Thank the gentlemen.

The Chairwoman now recognizes Mr. Ramotowski.

**STATEMENT OF EDWARD J. RAMOTOWSKI, DEPUTY ASSISTANT SECRETARY, BUREAU OF CONSULAR AFFAIRS, U.S. DEPARTMENT OF STATE**

Mr. RAMOTOWSKI. Thank you, Madame Chairwoman, Ranking Member Cuellar, and distinguished Members of the subcommittee.

As a consular officer with 26 years of experience in the U.S. Foreign Service, it is a solemn occasion for me to testify here today on the 11th anniversary of the September 11 attacks. I thank you for the opportunity to update you on how we continue to improve visa security to prevent such an attack from ever taking place again.

Our highest priority is the safety of American citizens at home and abroad. Together with our partner agencies, we build a layered visa and border security screening system, resting on technological advances, biometric innovations, consular interviews, expanded data sharing, and improved consular training.

The Department of State is constantly developing, implementing, and refining an intensive visa application and screening process. This process incorporates personal interviews in most cases and multiple biographic and biometric checks, supported by a sophisticated global information technology network.

We share this data among the Department and Federal law enforcement and intelligence agencies. Security remains our primary mission.

For us, every visa decision is a National security decision. Our electronic visa applications provide consular and fraud prevention officers, as well as our intelligence and law enforcement partners, the opportunity to analyze an applicant's data in advance of the visa interview, so that these partners may detect potential non-biographic links to derogatory information.

We are currently working with our partners on two major initiatives to screen more of this data with the law enforcement and intelligence communities, and make the visa system even more secure.

In addition to these biographic checks, the Department screens the fingerprints of visa applicants against DHS and FBI databases, and uses facial recognition technology to check applicants against

a watch list of photos obtained from the Terrorist Screening Center, as well as visa applicant photos contained in our Consular Consolidated Database.

Other agencies access our large database of visa information for security screening, law enforcement, and counter-terrorism purposes. We specifically designed our systems to facilitate comprehensive sharing.

We cooperate with law enforcement and intelligence agencies, and benefit from their capabilities and resources. This is most dramatically evident in the continuous vetting of visa holders, so that derogatory information that surfaces after a visa is issued is promptly reviewed, and the visa revoked, if warranted, by a dedicated revocation unit on 24/7 basis.

More than 8,000 visas have been revoked under the Continuous Vetting Program since 2010.

Consular officers are also thoroughly trained prior to making visa decisions. Each officer completes our consular course, which has a strong emphasis on border security and fraud prevention, and includes in-depth training on interviewing and name-checking techniques.

Officers also receive continuing education in all of these disciplines throughout their careers. On your next trip abroad, I would encourage you and all Members of the committee to visit the consular sections of the U.S. embassy or consulate to see these procedures first-hand and to observe how our dedicated consular personnel are carrying out their border security responsibilities.

Distinguished Members of the committee, our unique layered approach to border security screening, in which each agency applies its particular strengths and expertise, best serves our border security agenda, while furthering compelling U.S. interests in legitimate travel, trade promotion, and the exchange of ideas.

The United States must protect and advance all of these interests to guarantee our long-term security.

Thank you again for the opportunity to appear today. I am ready to answer your questions.

[The prepared statement of Mr. Ramotowski follows:]

PREPARED STATEMENT OF EDWARD J. RAMOTOWSKI

SEPTEMBER 11, 2012

Good morning Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee. It is a solemn occasion for me to testify here today on the 11th anniversary of September 11. I thank you for calling this hearing today, and for your unwavering commitment to visa security and prevention of terrorist travel.

The Department of State (the "Department") remains dedicated to the protection of our borders, and has no higher priority than the safety of our fellow citizens at home and abroad. We are the first line of defense in border security, because the Department is often the first U.S. Government agency to have contact with foreign nationals wishing to visit the United States. Since the terrorist attacks of September 11, 2001, we and our partner agencies have built a multi-faceted security screening process that extends our ability to review traveler information well before any potential threat reaches our borders. The lessons learned from that tragic day and subsequent terrorist attempts have not been ignored.

One of the most important improvements since 2001 is the enormous expansion of interagency cooperation, information sharing, and teamwork. Multiple Federal agencies responsible for border security, including the Department, share increasing amounts of data and coordinate lookout and screening activities. Likewise, we see

today an unprecedented level of information sharing with like-minded foreign governments. We and our partner agencies are committed to a layered approach to border security. This approach enables the U.S. Government to track and review the visa eligibility and status of foreign visitors from their visa applications throughout their travel to, sojourn in, and departure from, the United States.

SECURITY IMPROVEMENTS IN THE VISA APPLICATION PROCESS

Often, a foreign visitor's first step in traveling to the United States is applying for a visa at a U.S. embassy or consulate abroad. The Department has built a visa system that leverages state-of-the-art technology, extensive information sharing, highly skilled and trained consular officers, and interagency cooperation to facilitate legitimate travel and trade without compromising our Nation's security.

The Department constantly refines and updates the technology that supports the adjudication and production of U.S. visas. Under the Biometric Visa Program, before a visa is issued, the visa applicant's fingerprints are screened against two key databases. The first database is the Department of Homeland Security's (DHS) Automated Biometric Identification System (IDENT), which has a watch list containing available fingerprints of terrorists, wanted persons, and immigration law violators, as well as the entire gallery of more than 100 million individuals who have applied for visas, immigration benefits, and admission to the United States under the Visa Waiver Program (VWP), to combat identify fraud. The second database is the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS), which contains more than 50 million criminal history records. More than 10,000 matches of visa applicants with records on the IDENT watch list are returned to posts every month, normally resulting in visa refusals. In 2011, IAFIS returned more than 66,000 criminal arrest records to posts.

The Biometric Visa Program partners with DHS' US–VISIT Program to enable Customs and Border Protection (CBP) officers at ports of entry to match the fingerprints of persons entering the United States with the fingerprints that were taken during the visa application process at overseas posts and transmitted electronically to DHS IDENT. This biometric identity verification at ports of entry has essentially eliminated the previous problems of counterfeit and photo-substituted visas, as well as the use of valid visas by imposters.

The Department was a pioneer in the use of facial recognition techniques and remains a leader in operational use of this technology. Consular officers use facial recognition technology to screen all visa applicants against a watch list of photos of known and suspected terrorists obtained from the FBI's Terrorist Screening Center (TSC), as well as the entire gallery of visa applicant photos contained in the Department's Consular Consolidated Database (CCD). Currently, more than 109 million visa applicant photos are enrolled in our facial recognition database. Facial recognition screening has proven to be effective in combating identity fraud.

The on-line DS–160 non-immigrant visa application form is used worldwide, and we currently are piloting the on-line DS–260 immigrant visa application form. These new on-line forms provide consular and fraud prevention officers the opportunity to analyze data in advance of the visa interview, enhancing their ability to make decisions. The on-line forms offer foreign language support but applicants must respond in English, to facilitate information sharing between the Department and other Government agencies, who are able to view visa application data in foreign and domestic locations.

All visa applicants are checked against our automated Consular Lookout and Support System (CLASS), which contains 27 million records of persons found ineligible for visas, or against whom potentially derogatory information exists. CLASS employs strong, sophisticated name-searching algorithms to ensure matches between names of visa applicants and any derogatory information contained in CLASS. This robust searching capability has been central to our procedures since automated lookout system checks were mandated following the 1993 World Trade Center bombing. We use our significant and evolving experience with searching mechanisms for derogatory information to improve the systems for checking our visa issuance records constantly.

The amount of information contained in CLASS has grown more than 400 percent since 2001—largely the result of improved sharing of data among the Department, Federal law enforcement agencies, and the intelligence community. Almost 70 percent of CLASS records come from other agencies, including information from the FBI, DHS, DEA, and intelligence from other agencies. CLASS contains unclassified records on known or suspected terrorists (KSTs) from the Terrorist Screening Database, which is maintained by the TSC, and holds unclassified data on KSTs nominated by all U.S. Government sources. We also run all visa applicants' names

against the CCD in order to detect and respond to derogatory information regarding visa applicants and visa holders. The CCD contains more than 143 million immigrant and nonimmigrant visa records going back to 1998. A system-specific version of the automated CLASS search algorithm runs the names of all visa applicants against the CCD to check for any prior visa applications, refusals, or issuances.

In 2011, we deployed the Enterprise Case Assessment Service, a visa fraud tracking tool that provides a platform to store fraud-related research that used to be stored outside of consular systems. Should fraud be confirmed during the course of a visa interview, consular officers can record that data in this tool, and it will be permanently available to consular officers worldwide should the referenced individual re-apply for a visa. Future iterations of this tool will track fraud in other consular services, such as U.S. passport applications, and will enable us to track the activities of third-party document vendors and visa fixers.

INNOVATIONS IN THE SECURITY ADVISORY OPINION PROCESS

The Department's Security Advisory Opinion (SAO) mechanism provides consular officers with the necessary advice and background information to adjudicate cases of visa applicants with possible terrorism or other security-related ineligibilities. Consular officers receive extensive training on the SAO process, including modules on cultural and religious naming conventions, which assist them in identifying applicants who require additional interagency vetting. The SAO process requires the consular officer to suspend visa processing pending interagency review of the case. Most SAOs are triggered by clear and objective circumstances, such as CLASS name check results, nationality, place of birth, or residence.

In addition, in cases where reasonable grounds exist regardless of name check results, consular officers may suspend visa processing and institute SAO procedures if they suspect that an applicant may be inadmissible under the security provisions of the Immigration and Nationality Act (INA).

In the last quarter of 2012, in conjunction with our interagency partners, we will pilot major improvements to the way we process SAO requests. These changes will not only broaden our applicant screening for possible terrorist connections, but will also greatly enhance our ability to weed out false matches and more effectively focus vetting resources.

CHANGES TO THE VISAS VIPER PROGRAM

Our overseas posts provide information on foreign nationals with possible terrorist connections through the Visas Viper reporting program. Following the December 25, 2009 attempted terrorist attack on Northwest flight 253, we strengthened the procedures and content requirements for Visas Viper reporting. Chiefs of Mission are responsible for ensuring that all appropriate agencies and offices at post contribute relevant information for Viper nominations. These enhanced Visas Viper directives also included guidance on advanced name searches to identify information regarding previous or current U.S. visas, which must be included in Visas Viper cables; instructions regarding procedures and criteria used to revoke visas; and reiterated guidance on consular officers' use of the discretionary authority to deny visas under section 214(b) of the INA, with specific reference to cases that raise security and other concerns. Instruction in appropriate use of this authority has been a fundamental part of consular officer training for several years.

CONTINUOUS VETTING

The Department has been continuously matching new threat information with our records of existing visas since 2002. We have long recognized this function as critical to the way we manage our records and processes. This system of continual vetting evolved as post-9/11 reforms were instituted, and is now performed in cooperation with the TSC. All records added to the Terrorist Screening Database are checked against the CCD to determine if there are matching visa records. Matches are sent electronically from the Department to TSC, where analysts review the hits and flag cases for possible visa revocation. In addition, we have widely disseminated our data to other agencies that may wish to learn whether a subject of interest possesses a U.S. visa.

Cases under consideration for revocation are forwarded to the Department by our consular offices overseas, CBP's National Targeting Center (NTC), and other U.S. Government entities. As soon as information is established to support a revocation (i.e., information that could lead to an inadmissibility determination), a "VRVK" entry code showing the visa revocation is added to CLASS, and to biometric identity systems. This information is shared immediately with the DHS lookout systems used for border inspection and vetting. As part of its Pre-Departure and Immigra-

tion Advisory Programs, CBP uses these VRVK records, among others, to recommend that airlines not board certain passengers on flights bound for the United States.

The Department receives daily requests to review and, if warranted, revoke visas from aliens for whom new derogatory information has been discovered since the visa was issued. Our Operations Center is staffed 24 hours a day, 7 days a week, to address urgent requests, such as when a potentially dangerous person is about to board a plane. In those circumstances, the State Department can and does use its authority to revoke the visa prudentially, and thus prevent the individual from boarding.

The Department has broad and flexible authority to revoke visas and we use that authority widely to protect our borders. Since 2001, the Department has revoked approximately 62,000 visas for a variety of reasons, including nearly 6,000 for suspected links to terrorism. Most revocations are based on new information that has come to light after visa issuance. Because individuals' circumstances change over time, and people who once posed no threat to the United States can become threats, revocation is an important tool. We use our authority to revoke a visa immediately in circumstances where we believe there is an immediate threat. At the same time, we believe it is important not to act unilaterally, but to coordinate expeditiously with our National security partners in order to avoid possibly disrupting important investigations. Individuals whose visas are revoked may reapply at a U.S. embassy or consulate abroad; their reapplication would be subject to complete interagency security vetting to determine their eligibility for a visa.

THE ASSISTANT REGIONAL SECURITY OFFICER, INVESTIGATOR PROGRAM

The Bureau of Diplomatic Security (DS) Assistant Regional Security Officer, Investigator (ARSO–I) Program adds an important law enforcement element to the Department's visa security capabilities. There are currently 105 ARSO–I positions approved for 93 consular sections overseas, specifically devoted to working with our foreign law enforcement partners to combat travel document fraud and other law enforcement issues. These highly trained law enforcement professionals add another important dimension to our border security efforts, and we are working with DS to identify additional locations for ARSO–I placement.

ARSO–Is train our foreign partners in the recognition of fraudulent travel documents and work closely with immigration and airline security officials assigned at foreign airports. They teach courses at our International Law Enforcement Academies, networking with foreign law enforcement partners and learning about vulnerabilities in foreign visa and passport systems. DS agents share this information with each other, resulting in additional investigations and opportunities to shut down human smuggling and trafficking networks that could potentially be exploited by terrorists. ARSO–Is have trained over 50,000 foreign law enforcement personnel, resulting in stronger global enforcement efforts targeting illicit methods of travel.

ARSO–Is work very closely with consular fraud prevention managers, sharing information and participating in joint training sessions to ensure that adjudicating consular officers possess up-to-date information on fraud trends in their country. They are complemented by DS agents working domestically on visa and passport fraud criminal investigations and analysis. Investigations that originate overseas often have a U.S. nexus, and close collaboration between overseas and domestic DS agents has resulted in many U.S.-based prosecutions.

COOPERATION WITH THE VISA SECURITY PROGRAM

The Department of State believes that the Visa Security Program (VSP), under which DHS establishes Visa Security Units (VSU) staffed with U.S. Immigration and Customs Enforcement (ICE) special agents at certain overseas consular posts, is another valuable component of the U.S. Government's overall border security program. We have a close and productive partnership with DHS, which has authority for visa policy under section 428 of the Homeland Security Act, and are fully supportive of the mission and future of the VSP.

The VSP increases the utility of the visa application and interview processes to detect and combat terrorism, criminality, and other threats to the United States and the traveling public. ICE special agents assigned to VSUs provide on-site vetting of visa applications and other law enforcement support to our consular officers. When warranted, DHS officers assigned to VSUs will conduct targeted, in-depth reviews of individual visa applications and applicants prior to issuance, and recommend refusal or revocation of applications to consular officers. We work very closely with DHS to ensure to the maximum possible extent that no terrorist receives a visa or is admitted into our country.

As the VSP has matured over the past few years, VSU personnel have moved beyond a singular focus on visa application review. Working with their law enforcement colleagues assigned to our various missions, they have contributed their expertise and resources to enhance our response to all kinds of threats to the visa and immigration processes including human smuggling and trafficking.

In Washington, we work very closely with our VSP colleagues on day-to-day issues affecting the operations of the program, as well as longer-term issues related to the expansion of the program to select overseas posts. VSP officers in Washington review our visa databases and advise posts of emerging information about visa holders. Another important aspect of our Washington partnership is coordinating VSP expansion to more posts. The Department's Bureaus of Consular Affairs (CA) and Diplomatic Security (DS) have a Memorandum of Understanding (MOU) with ICE governing VSU-Department of State interactions with visa sections. This MOU outlines procedures for resolving the very few disputed visa cases that emerge from the VSU review process, and collaboration between ICE/VSU agents and their DS law enforcement colleagues assigned as Regional Security Officers (RSOs) or ARSO–Is.

Currently, 19 VSUs are active at posts in 15 countries. In administering and expanding the VSP, the Department works collaboratively with DHS, pursuant to an October 2004 MOU between the Department and the VSP on the "Administrative Aspects of Assigning Personnel Overseas," and National Security Decision Directive 38 (NSDD–38). This directive outlines factors to be considered by Chiefs of Mission when considering requests by a U.S. Government agency to create a new position at a post abroad. NSDD–38 gives Chiefs of Mission responsibility for the size, composition, and mandate of U.S. Government agency staff under his or her authority.

Before submitting an NSDD–38 request, ICE officials, with the support of senior Department officers from CA and DS, conduct a post-specific, on-site assessment. The visit provides an opportunity for the team to consult with officials at post to validate the interagency assessment of the risk environment, determine the feasibility and timing of establishing an office, and brief the Chief of Mission on the role of the VSU. In 2012, joint Department/DHS teams conducted assessment visits to two potential VSU sites, and follow-on NSDD–38 requests currently are under consideration by the Department of State.

LAYERED SECURITY AND DATA SHARING

As I have previously stated in my testimony, the Department embraces a layered approach to security screening. In addition to our support of the VSP, the Department and DHS have increased resources significantly, improved procedures, and upgraded systems devoted to supporting the visa function over the past 7 years. DHS receives all of the information collected by the Department during the visa process. DHS's US–VISIT is often cited as a model in data sharing because the applicant information we provide, including fingerprint data, is checked at ports of entry to confirm the identity of travelers. DHS has access to our entire CCD. A menu of reports tailored to the specific needs of each particular unit is supplied to elements within DHS, such as ICE's agents assigned to VSUs.

All of our visa information is available to other U.S. Government agencies for law enforcement and counterterrorism purposes, and our systems are specifically designed to facilitate tailored and comprehensive data sharing with our partners. We give other agencies immediate access to more than 14 years of visa data for these purposes, and they use this access extensively in the course of conducting law enforcement and/or counterterrorism investigations.

Working in concert with DHS, we proactively expanded biometric screening programs and integrated this expansion into existing overseas facilities. In partnership with DHS and the FBI, we established the largest fingerprint screening program on the globe. These efforts require intense on-going cooperation from other agencies. We successfully forged and continue to foster partnerships that recognize the need to supply accurate and speedy screening in a 24/7 global environment. As we implement process and policy changes, we are always striving to add value in both border security and in operational results. Both dimensions are important in supporting the visa process.

In addition, every post that issues visas has at least one fraud prevention officer and locally-employed staff devoted specifically to fraud prevention and document security. We have a large Fraud Prevention Programs office in Washington, which works closely with DS. We have fraud screening operations which use sophisticated database checks at the Kentucky Consular Center in Williamsburg, Kentucky, and the National Visa Center in Portsmouth, New Hampshire. Their role in flagging questionable applications and applicants who lack credibility, present fraudulent

documents, or give us false information adds a valuable dimension to our visa process.

## FACING THE TERRORIST THREAT

We face an evolving threat of terrorism against the United States, but the multi-agency team effort, based upon broadly-shared information, provides a solid foundation for securing U.S. borders. The people and tools we use to address this threat are sophisticated and flexible. The interagency community continues to automate processes to reduce the possibility of human error, and enhance our border security screening capabilities.

Our response to these threats accounts for the cultural and political environment in which they arise. Our officers are well-trained, motivated, and knowledgeable. Our information is comprehensive and accurate. Our criteria for taking action are clear and coordinated. The Department remains fully committed to fulfill our essential role on the border security team.

## ENHANCED COOPERATION WITH FOREIGN PARTNERS

The U.S. Government's information-sharing initiatives ensure that we and our international partners are in constant contact regarding the threat of terrorist travel. The Department plays a key role in all of these international initiatives.

Homeland Security Presidential Directive 6 (HSPD–6), among other things, called for enhancing information sharing with our foreign partners, starting with those countries participating in the Visa Waiver Program. Through July of this year, the Department, in collaboration with the TSC, has negotiated more than 40 agreements or arrangements facilitating the bilateral exchange of terrorism screening information. These agreements enhance the data in our U.S. Government's known or suspected terrorist watch list and strengthen our counterterrorism cooperation.

We also have entered into arrangements for the sharing of visa information with foreign governments, consistent with the requirements of section 222(f) of the INA. Since 2003, there have been arrangements in place with Canada for such sharing under certain circumstances. With DHS, the Department is participating in a pilot program, through the Five Country Conference (United States, Australia, Canada, New Zealand, and the United Kingdom) for identification of some travelers based on biometric matching. We are in negotiation with the governments of Canada and the United Kingdom for agreements that would provide a legal basis for us to implement arrangements for the automated sharing of visa refusal data and for systematic confirmation of an applicant's identity through biometric matching. We expect both agreements to be completed this year, and similar agreements with Australia and New Zealand in 2013.

We have been and remain a close partner of DHS in API and PNR discussions overseas, in particular with respect to the talks with the European Union leading to the PNR Agreement that entered into force on July 1, 2012. Together, all of these programs are helping achieve the goal of constraining terrorist mobility and ensuring the security of travelers. This is our obligation to the American people.

## CONCLUSION

The Department's border security agenda does not conflict with our support for legitimate trade and travel. In my testimony for your subcommittee and for the subcommittee on Travel and Tourism of the Senate Committee on Commerce, our message is the same: The United States' long-term interests and security are served by continuing the flow of commerce and ideas that are the foundations of prosperity and security. Exposing international visitors to American culture and ideals is the best way to decrease misperceptions about the United States. Fostering academic and professional exchanges keeps our universities and research institutions at the forefront of science and technology.

The Department continues to refine its intensive visa application and screening process requiring personal interviews, employing analytic interview techniques, incorporating multiple biographic and biometric checks, all supported by a sophisticated global information technology network. We have visa offices in virtually every country of the world, staffed by consular officers drawn from the Department's professional, mobile, and multilingual cadre of Foreign Service Officers. These officials are dedicated to a career of worldwide service, and provide the cultural awareness, knowledge, and objectivity to ensure that the visa function remains the front line of border security. Each officer's experiences and individual skill set are enhanced by an overall understanding of the political, legal, economic, and cultural development of foreign countries in a way that gives the Department of State a special expertise over matters directly relevant to the full range of visa ineligibilities.

The Department's global presence, foreign policy mission, and personnel structure give us singular advantages in executing the visa function throughout the world. Our authorities and responsibilities enable us to provide a global perspective to the visa process and its impact on U.S. National interests. The issuance and refusal of visas has a direct impact on our foreign relations. Visa policy quickly can become a significant bilateral problem that harms broader U.S. interests if handled without consideration for foreign policy equities. The conduct of U.S. visa policy has a direct and significant impact on the treatment of U.S. citizens abroad. We are in a position to anticipate and weigh all those factors, while always keeping border security as our first priority.

This concludes my testimony today. I will be pleased to take your questions.

Mrs. MILLER. Thank the gentlemen.

The Chairwoman now recognizes Mr. Edwards for his testimony.

**STATEMENT OF CHARLES K. EDWARDS, ACTING INSPECTOR GENERAL, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF HOMELAND SECURITY**

Mr. EDWARDS. Good morning, Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee. Thank you for inviting me to testify today regarding border security to detect and deter terrorist travel.

I will present the results of three reports that we issued in the past year on this topic. Specifically, we looked at resources and coordination among DHS agencies to screen foreign nationals and protect the border, controls that US–VISIT to identify potentially fraudulent attempt to enter the United States and TSA's implementation of the Secure Flight Program.

The infrastructure for securing our borders is layered. Federal entities such as the Department of State and DHS components like CBP, TSA, US–VISIT and ICE make vital contributions to border security. In addition, other Federal, State, and local entities play critical roles in this layered strategy.

However, technological issues, resource deficiencies and interagency coordination present significant challenges. For example, DHS officers at any of the 327 air, sea, and land border ports of entry have to access as many as 17 different DHS systems to verify the identity of foreign nationals and make admission decisions.

Some components have made progress in streamlining their systems. However, mobile devices used by some SBP officers and border patrol agents continue to lack adequate bandwidth and technology. This can hinder officers in the field attempting to fingerprint aliens or accessing law enforcement and immigrant databases.

In addition, long-standing mission overlap and inadequate information sharing between CBP and ICE agents at the Northern Border have sometimes led to duplication of efforts and concerns over officer safety. The Department concurred with five of the eight recommendations, and has implemented actions to address our findings.

DHS has even taken actions to close two of the three recommendations with which it did not concur. We expect the final recommendation to be closed next month. US–VISIT is designed to collect and analyze foreign nationals' biographic and biometric data and provide timely, accurate information to border enforcement officials to prevent entries of potentially fraudulent and dangerous individuals.

However, we found hundreds of thousands of instances where the same fingerprint was recorded in US–VISIT's database with sometimes as many as 14 different names and dates of birth. The vast majority of this faulty data is attributable to data entry errors in the name and date fields.

However, US–VISIT officials were unable to quantify how many of those inconsistencies came from individuals purposefully presenting fraudulent information at the border. Our report identified a number of instances where individuals with derogatory information, such as criminal aliens, supplied different biographic information to CBP officers in an attempt to enter the United States.

These individuals were not flagged in the IDENT Database. US–VISIT concurred with our recommendations to improve procedures to target, identify fraud.

Another pillar in the fight against terrorism is TSA's Secure Flight Program. Through this program, TSA assumed from commercial operators the matching of passenger names against the terrorist watch list. If passenger information matches closely enough against the watch list record, a TSA analyst must complete a manual review of that passenger's record.

Unless the match is resolved, the boarding pass cannot be printed until the passenger provides identification to the aircraft operator and TSA. TSA may also may require a passenger to undergo additional screening at a secure checkpoint or deny that person access beyond the security area altogether.

The standardization affected by Secure Flight has resulted in more consistent watch list matching process. However, Secure Flight's watch list matching results are sometimes disrupted by DHS and aircraft operator system outages. In some instances, aircraft operators have overridden TSA controls and allowed inhibited individuals to board the aircraft.

In response to our recommendations, TSA has taken steps to address these issues.

Madam Chairwoman, this concludes my prepared remarks. I thank you again for the opportunity to testify before this committee. I would be happy to answer any questions you or other Members might have. Thank you.

[The prepared statement of Mr. Edwards follows:]

PREPARED STATEMENT OF CHARLES K. EDWARDS

SEPTEMBER 11, 2012

Good morning Chairwoman Miller, Vice Chairman Quayle, Ranking Member Cuellar, and distinguished Members of the subcommittee. I am Charles K. Edwards, acting inspector general of the Department of Homeland Security (DHS). Thank you for inviting me to testify about the results of our work on border security. I will present the results of three recent reports on DHS' implementation—along with other departments and agencies—of various programs aimed at securing our border and preventing terrorist travel.[1] Specifically, I will address: (1) DHS screening of foreign nationals, as well as the cooperation, resources, and technology necessary to share information and safeguard our borders; (2) the United States Visitor and Immigrant Status Indicator Technology Office's (US–VISIT's) oversight of biographic and biometric data for foreign nationals entering the United States; and (3) the

[1] The information provided in this testimony is contained in the following reports: Information Sharing on Foreign Nationals: Border Security (OIG–12–39); US–VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities (OIG–12–111); and Implementation and Coordination of TSA's Secure Flight Program (OIG–12–94).

Transportation Security Administration's (TSA's) implementation of the Secure Flight program.

MULTIPLE DEPARTMENTS AND AGENCIES PLAY CRUCIAL ROLES IN BORDER SECURITY

The security infrastructure at U.S. borders is layered and the Department of State (State), DHS components, and other Federal, State, local, Tribal, and private entities play critical roles in securing our border. For example, State Department consular personnel review the visa applications of all individuals traveling to the United States from countries where visas are required. State approves visas only after checking the individual's fingerprints against previous biographic records associated with those fingerprints to ensure that the individual has not previously used different biographic information to enter the United States. TSA performs passenger watch list matching for all covered flights into, out of, within, and over the United States. U.S. Customs and Border Protection (CBP) analyzes cargo and passenger manifests to identify higher risk matters for subsequent examination, and CBP immigration Advisors provide real-time assistance to foreign authorities at some foreign airports.

In addition to control procedures that occur prior to foreign nationals entering the United States, other Federal entities have control procedures designed to identify potential criminal behavior at entry to the United States or subsequently, in order to flag individuals for future apprehension. CBP officers at ports of entry check travel documents to identify potential fraudulent or stolen passports, visas, or other travel documents before admitting an individual to enter the United States. Even after entry, US–VISIT and other DHS data systems play a crucial role in processing data captured by numerous agencies to identify and flag potential identity fraud or individuals who have overstayed their visas. Multiple layers of effective security programs and coordination among agencies are crucial to protecting our Nation.

SCREENING OF FOREIGN NATIONALS AND INFORMATION SHARING [2]

We identified resource and technological difficulties facing DHS' border security programs in screening foreign nationals, as well as challenges in coordinating among DHS components.

*Resource and technological difficulties*.—DHS officers at any of the 327 air, sea, or land border ports of entry have to access as many as 17 different DHS systems to verify the identity and evaluate the admissibility of foreign nationals seeking to enter the United States. This process is labor-intensive, and the inefficiency of using multiple data systems hinders border security officers in their efforts to verify or eliminate links to possible terrorism or other derogatory information. While CBP and U.S. Immigration and Customs Enforcement (ICE) have developed more streamlined software to conduct immigration inspections, apprehension, and enforcement, DHS officers with more complex border security caseloads still face challenges in data systems. In addition, some ports of entry, land, and maritime border operations had unmet infrastructure needs. For example, at some land border ports of entry, limited direct access to law enforcement, intelligence, and immigration databases and high-speed internet connections had a negative effect on the operations of these locations. Some CBP Officers who conduct outbound screening—and most Border Patrol Agents in the field—use only mobile devices that lack the bandwidth and access to multiple databases that desktop terminals provide.

*Information Sharing and Coordination*.—Our Inspection Report 12–39 describes challenges presented by the long-standing mission overlap between CBP and ICE agents at the Northern Border. The intersection of their responsibilities, along with inadequate information sharing, has sometimes led to duplication of missions and concerns over officer safety. These problems also hindered the effectiveness and efficiency of operations to screen and process foreign nationals. We determined that CBP and ICE do not always share all information and intelligence related to open investigations, even when the origin of the investigation comes from both agencies. Further, the data systems used by CBP and ICE are not designed for information sharing on investigations, or to identify operations that may overlap between the two agencies. DHS-level guidance is necessary to provide clarity on missions and priorities for law enforcement agencies that share overlapping mandates, such as ICE and CBP.

[2] Information Sharing on Foreign Nationals: Border Security (OIG–12–39).

US–VISIT'S OVERSIGHT OF TRAVELER DATA [3]

The Automated Biometrics Identification System (IDENT) maintained by US–VISIT contains hundreds of thousands of discrepant records. We also determined that the identity resolution processes at US–VISIT are manual and not specifically targeted to identifying individuals who may have presented fraudulent identities to attempt to enter the United States.

IDENT contains biographic and biometrics information collected by various agencies including State, ICE, CBP, U.S. Customs and Immigration Services (USCIS), and the Federal Bureau of Investigations (FBI). Each time an international traveler passes through a United States port of entry, US–VISIT checks the person's biometrics, i.e., fingerprint and/or picture, against a biometric watch list of more than 6.4 million known or suspected terrorists, criminals, and immigration violators. In addition, US–VISIT checks the foreign visitor's fingerprint along with their permit and/or other documents against a number of systems to verify an individual's identity and authenticate travel document. These efforts at US–VISIT assist CBP officers make a final determination as to whether the individual should be admitted.

*Oversight of Overstays and Identity Resolution*.—According to US–VISIT officials, they have identified individuals who have overstayed visas by comparing visa information against entry and departure data, and established overstay lookouts so CBP officers and Department of State personnel can be warned of potential overstays seeking reentry to the United States. In fiscal year 2011, US–VISIT referred more than 900 visa overstay leads per week to ICE. US–VISIT also provides other Federal law enforcement and intelligence community with historical biographic and biometric information in the course of their investigations.

With respect to identity resolution, US–VISIT reviews records of foreign nationals entering and exiting the United States where different biographic data were associated with the same biometrics. This process involves US–VISIT analysts manually reviewing entry records to determine whether biographic information was input incorrectly at the point of collection, or whether fraud may have occurred. For example, analysis of discrepant data may reveal that a husband and wife had their passports switched during entry, a traveler's first and last name was switched at entry, or a traveler's birth date was recorded using different day and month format.

*Procedures Targeting Potential Identity Fraud Needs Improvements*.—The manual review process presents challenges considering the large volume of data that exist on travelers who sought entries into the United States. Specifically, our analysis of data from IDENT identified more than 800,000 instances affecting 375,000 individuals where the name and/or date of birth did not match other records with the same fingerprint identification number. These hundreds of thousands of records with inconsistent biographic data limit the effectiveness and efficiency of using biometrics to identify and prevent the use of fraudulent identities at U.S. ports of entry. According to US–VISIT officials, US–VISIT manually reviews IDENT encounters with multiple biographic records to identify potential identity fraud. However, US–VISIT's current identity resolution effort is not designed to specifically target individuals who are using multiple identities to enter the United States. Since 2005, US–VISIT analysts have referred only two instances of biographic fraud to ICE.

*Data Inconsistencies Hinder Oversight Effectiveness*.—Most of the multiple identities appear to be data integrity errors. For example:

- Test data existed in the alien encounter information that US–VISIT provided to us. In a number of instances, we reviewed records with the same fingerprint number but with fictitious names such as "Mickey Mouse" and "Jarvis Sample."
- In a number of instances, the same set of fingerprints was used to record the names of as many as seven different individuals.
- Nearly 400,000 records for women have different last names for the same first name, date of birth, and fingerprint. According to US–VISIT officials, these instances are likely women who changed their names after a marriage.

However, US–VISIT was unable to quantify how much of the biometric/biographic inconsistencies can be attributed to data entry and other identifiable errors, and how much occurred because of intentional fraud by individuals who used different biographical data to attempt illegal entry.

*Examples of potential fraud*.—Our analysis of IDENT identified that individuals used different biographic information at ports of entry after they had applied for a visa under a different name or been identified as a recidivist alien. These multiple biographic identities were not flagged in IDENT. For example:

[3] US–VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities (OIG–12–111).

- A male who used two different names and dates of birth to attempt to enter the United States in 2008 and 2011 was identified as a repeated criminal (recidivist) alien.
- A female who was identified as a recidivist alien in 2008 used different biographic data to attempt to enter the United States, once in 2009 and twice in 2011.
- A female who was identified as a recidivist alien in 2006 attempted to enter the country on three visits in 2009, 2010, and 2011 under variations of the same name.

Although the more than 800,000 instances represented less than 1 percent of overall IDENT encounter data we received from US–VISIT, the potential risk can be significant. Critical work performed by CBP and State mitigates some of the security risks. However, without a process to distinguish between errors and potential fraud quickly, US–VISIT is limited in its ability to flag identity fraud, and therefore help border enforcement agencies prevent improper entries into the United States.

## TSA'S IMPLEMENTATION OF THE SECURE FLIGHT PROGRAM [4]

Through the Secure Flight program, TSA assumed from commercial operators the performance of passenger watch list matching for all covered flights into, out of, within, and over the United States. Aircraft operators are required to submit passenger data to Secure Flight prior to flight departure for advanced passenger prescreening. Secure Flight implementation has resulted in a more consistent watch list matching process. However, DHS and aircraft operator system outages sometimes disrupt the process.

*More Consistent Watch List Matching*.—TSA requires aircraft operators to transmit airline passenger information including name, gender, passport number (if applicable) and date of birth to Secure Flight. Passenger information is submitted 72 hours prior to flight departure, and a high-priority queue has been established for reservations created subsequently. TSA matches the passengers' biographic information against the Terrorist Screening Database and the No-Fly and Selectee subsets. If the information matches closely enough against a watch list record, the Secure Flight system flags the record for manual review by a TSA analyst. If the analyst needs more information, the boarding pass is "inhibited"—it cannot be printed until the passenger provides identification to the aircraft operator and TSA. Based on the review, TSA may clear the individual. Alternatively, TSA may provide for additional screening at a security checkpoint, or deny boarding or authorization to enter a U.S. airport's sterile area.

Because all airlines are required to use the same process, Secure Flight has provided a more consistent watch list matching process for both TSA and passengers. However, aircraft operators have the ability to override inhibited boarding passes. When this occurs, inhibited individuals who have not yet been cleared by Secure Flight may not be handled appropriately before entering an airport's sterile area or boarding an aircraft. In its response to our report, TSA said that they have taken steps to identify how and when aircraft operators inappropriately engaged in overrides, ensure screening is performed when overrides are identified, and launch compliance investigations.

*Secure Flight Sometimes Disrupted by System Failures*.—Secure Flight's watch list matching results are sometimes disrupted by DHS and aircraft operator system outages. Outages may require aircraft operators to revert to alternative procedures that may include pre-Secure Flight watch list matching procedures and protocols. TSA has established procedures to identify and resolve outages. Secure Flight has also taken steps to address these disruptions through operation center and system redundancy.

Our reports have described the work and coordination of agencies within and outside the Department of Homeland Security that play an important role in deterring terrorist travel. Because of the hard work of these entities, we have identified and stopped terrorist acts before they have occurred. However, our reports have also identified a number of areas, including identification of fraudulent identities, system interfaces, and increased coordination, where agencies can make further improvements to help ensure the efficiency, accuracy, and effectiveness of our complex border security system.

Mr. Chairman, this concludes my prepared remarks. I welcome any questions that you or the Members of the subcommittee may have.

---

[4] Implementation and Coordination of TSA's Secure Flight Program (OIG–12–94).

Mrs. MILLER. Thank you all very much. I certainly appreciate your service to the country, first of all. One of the things that I think we all learned from the 9/11 Commission recommendation—well, there were a number of excellent recommendations in this document. I tell you, in our office, we don't regard this as shelfware. We use it all the time. We are constantly referencing it on various points.

But certainly one of the things that has always stuck in my mind is that we need to move from the need-to-know to the need-to-share information. When we talk about visa overstays or problems with the visa application process that we have had in our Nation, first of all, let us all recognize that we have made unbelievable positive strides forward since 9/11 in our processes.

But the largest room is always a room for improvement, I suppose. I think it is particularly so when—I mentioned about the Christmas day bomber in my opening remarks. But, you know, with the kind of threat that we face, these enemies of freedom are looking at a battlefield in different optics, I suppose you could say, than we ever have before. They see the battlefield in a very asymmetrical way.

Certainly on that particular day, the Christmas day bomber saw the battlefield as seat 19A on that Northwest flight. That was the battlefield for him.

I know that we had a problem in the visa application process with that particular individual because of a spelling error. That was brought to everybody's attention, et cetera. Subsequently, since that time, we have had, again, tremendous strides forward, I think, in our visa processes.

We are doing the vetting against the watch listing. You are doing your initial application checks, et cetera. So I guess my question is—and I know the revocation process has significantly increased since that time as well, all to the good.

I guess my question would be, if you could flesh out a bit how something like that had happened, how it hopefully would not happen in the future, as you think about, again, the need-to-know to the need-to-share information on how cooperation is happening in a better way with the various agencies, the Department of State, CBP, your overseas consular applications, et cetera.

I am not sure who I am addressing this to.

Ms. WALTHER. I am happy to kick it off.

Mrs. MILLER. Okay.

Ms. WALTHER. The interagency conducted a complete review following the events 12/25 in 2009, and took several significant steps following that event. One of our largest was the robust interagency process to revise the criteria for nominations to the watch list to close gaps.

We also have 100 percent vetting of all commercial airline passengers today through Secure Flight. CBP also vets on a recurrent basis all visa holders. CBP's pre-departure program pushed back the vetting of passengers before they board a plane.

As an international effort, working with our international partners, DHS worked with the International Civil Aviation Organization, looking at a global framework for how we look at aviation security. That framework was supported by nearly 190 countries.

So you can see that in the interagency, as well as with our international partners, we continue to be aggressive. We will not stop until we prevent terrorist attacks to the United States.

Mrs. MILLER. Very good.

Does anyone else have any follow-on to that?

Mr. RAMOTOWSKI. Yes, I would just like to add that from the perspective of the State Department, we have significantly strengthened our Visas Viper procedures, which is the State Department's method of reporting individuals for watch listing. At the time of the 12/25/09 incident, as my colleague has stated, the interagency watch-listing guidance did not permit for Mr. Abdulmutallab to be watch listed. We have changed that.

The Department also acts immediately whenever a Visas Viper message arrives with an individual who currently possess a valid visa. That visa will be revoked unless a law enforcement or intelligence agency asks us not to.

Mrs. MILLER. I appreciate that.

The Chairwoman now recognizes our Ranking Member.

Mr. CUELLER. Thank you, Madam Chairwoman. Just a quick statement, because as you know, we will be cutting the committee down because we have the 9/11 remembrance there at the Capitol steps. We certainly don't want to be late for that.

Let me just say this: I think we are all on the same page. So we have got to do everything possible to make sure we don't let another group or individual attack the United States as we saw back in 9/11/2001. But at the same time as we do that, we have to make sure that we don't let the pendulum swing over so much to the other side where we restrict our own freedoms and our own economic freedoms also, in the sense that we got to find that balance between security and making sure that the legitimate trade, tourism, people coming into the United States are coming in.

I would ask you all that as you look at that, you look at a couple of things. One is the efficiencies that you all are looking at and finding ways to get more efficient. You know, still providing security but the efficiencies, so we minimize the impacts to the legitimate trade and tourism, people coming in.

The other thing is, keep in mind that a couple of years ago, just 2 years ago, we passed the modernization of the performance based act that we have here in the Congress. I would ask you—if you are not familiar with that, I would ask you to look at that, because as time goes on, we are going to be looking at more the performance, not measuring activity, but performance, measuring the results.

We give you $1; what do we get for $1? What does the taxpayer get back? So I would ask you, as you are looking at your great job that you are doing, and we appreciate what you all are doing, is to look at the efficiencies, trying to find the balance in the work that you are doing.

I know some of you all are law enforcement. I have three brothers that are law enforcement. I got a brother who is a border sheriff down there on the border. I understand law enforcement is so important to us. But at the same time, just keeping in mind that you still have an impact on business, on tourism and on the people that are trying to do the legitimate trade and tourism over here.

So I would ask you—and again, I guess I would turn from a question a statement. I would only ask you to please keep that in mind as you do your job. You do it in a good way. I salute all the men and women that are doing your job for the State Department, CBP, and the inspector general, and the other folks working together.

But just don't lose sight of the efficiencies, maximizing the taxpayers' dollars, finding the balance in security and trade and tourism. If we do that, I think our country will remain secure, but still remain prosperous and free.

Thank you so much. Again, to all of you, I thank you for what you and your men and women do. Thank you so much.

Mrs. MILLER. I thank the Ranking Member. I thank all the committee individuals for being here today, my colleagues. As was said, we have a remembrance ceremony on the steps of the Capitol in a very few short minutes. I think that will serve to focus all of our attention on what happened that terrible day 11 years ago when the enemies of freedom attacked our Nation, and they really tried to get us to retreat from freedom.

In that, they failed miserably. We have seen in the last 11 years, the sons and daughters of America rise up and defend our freedoms, our liberty, our democracy. What is happening even here today with this hearing is a very vivid demonstration I think of the unity of purpose of every American to make sure that we always advance the cause of freedom, not only here in the United States domestically, but certainly we are a society that takes that message across the globe. We intend to continue to do so.

As I say, they failed very miserably. Today is a way for us certainly to commemorate those innocent Americans that were murdered by these cowardly terrorists. We all have a unity of purpose to make sure that we do protect our homeland, harden our defenses.

Again, I appreciate all of the witnesses being here today.

With that, the subcommittee stands adjourned.

[Whereupon, at 10:43 a.m., the subcommittee was adjourned.]

# APPENDIX

---

QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR KELLI ANN WALTHER

*Question 1a.* The DHS Inspector General's August 2012 report regarding US–VISIT found instances where intersecting responsibilities and inadequate information sharing between CBP and ICE had hindered operations to screen and process foreign nationals as well as concerns over officer safety. The OIG asserts that these issues cannot be corrected without DHS-level guidance in order to provide clarity on missions and priorities.

As a result of the OIG August report, how does DHS plan to implement changes in order to alleviate on-going overlapping responsibilities between CBP and ICE related to preventing terrorist travel?

Answer. The OIG determined that DHS has invested considerable resources to improve staffing and infrastructure to facilitate information sharing. DHS continues to take steps to further strengthen information sharing, communication, and coordination in this area, and address the OIG recommendations.

A key layer in the DHS multi-layer approach to preventing terrorist travel is to identify persons that may pose a risk to U.S. citizens or whose entry may violate U.S. law, before they reach the United States. U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) have complementary, coordinated roles in the prevention of terrorist travel; both CBP and ICE share information with partners regarding foreign nationals who seek to enter the United States.

An example of a joint effort between ICE and CBP is the coordinated screening of visa applications. The ICE Visa Security Program (VSP) currently screens and vets select non-immigrant visa applications prior to visa adjudication and issuance and CBP conducts recurrent vetting of all valid visas against newly identified derogatory information. To enhance visa security, DHS, ICE, CBP, and the Department of State (DOS) are collaboratively developing an automated visa screening process that will enable DHS entities to identify derogatory information relating to all visa applicants prior to their application being adjudicated by a consular officer. This process will inform and be used in conjunction with the current DOS Security Advisory Opinion (SAO) and Advisory Opinion (AO). DHS internal cooperation and efficiency with respect to issued visas and revocation recommendations is also expected to continue to improve and be expanded in conjunction with the new process. Additionally, DHS, DOS, and the intelligence community are working to establish a process to screen all visa applications against intelligence information provided by the interagency prior to visa issuance. This proposed coordinated review process includes the capability to utilize rule-based vetting methodologies, to provide detailed case notes and justification for any recommendations related to visa issuance, and to recommend applicants for targeted interviews.

Employing ICE VSP authorities, leveraging CBP expertise and authorities, and utilizing current information technology platforms to screen pre-adjudicated visa applications and expand the scope of recurrent visa vetting significantly enhances the U.S. Government's anti-terrorism efforts by adding another layer of security to the process while further extending our borders outward.

*Question 1b.* Has DHS established a time line to implement these changes? Please explain.

Answer. As explained in the prior response, the multi-layer approach utilized by DHS ensures that the missions and operations of the Department complement, rather than overlap each other. In an effort to enhance visa security measures, representatives from ICE, CBP, and DOS are developing PATRIOT (Pre Adjudicated Threat Recognition Intelligence Operations Team), a joint project that will revolutionize the visa process by both automating the screening of pre-adjudicated visa ap-

plicants against DHS holdings and collectively leveraging the respective ICE and CBP authorities relating to visas.

When fully operational PATRIOT will have the capability to screen and vet all non-immigrant visa's worldwide daily (pre-adjudicative) and provide derogatory findings to all 73 HSI attaché offices in addition to all U.S. Embassies/Consulates without an HSI presence. Complete operational capabilities are anticipated to be completed within 2 years from version 2.0 release in early January 2013.

The release of version 2.0 in January 2013 will provide 100 percent pre adjudicative screening and vetting capabilities to the 19 existing HSI attaché offices with visa security operations.

*Question 2a.* The DHS Inspector General's August 2012 report regarding US–VISIT raises serious questions regarding the integrity of the data used by the US–VISIT system. While some of the discrepancies may be due to data entry errors, it seems that some travelers may be exploiting the overburdened manual entry system.

What process is in place to target individuals who are using multiple identities to enter the United States?

Answer. The U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT) Program received the OIG's full 825,000 instances where the OIG determined that the same fingerprints were associated with different biographic data and will review the full data set for potential fraud. Fraud, in this context, addresses attempts by individuals to enter the country rather than successful admissions.

US–VISIT proactively reviews IDENT records to identify potential fraud by individuals attempting to enter the United States or obtain immigration benefits. If an individual is suspected of fraud, he or she is referred to the appropriate law enforcement agency and placed on the watch list for appropriate action. Additionally, a TECS record is created so that the agency/stakeholders encountering the subject can review the information and make a determination on a course of action. Case information may also be forwarded to other agencies for possible fraud notification.

In addition, US–VISIT searches for discrepant biographical information corresponding to a single Fingerprint Identification Number, or FIN, based on certain other system identifiers. US–VISIT reviews encounters with biographical discrepancies to determine if there was a typographical error, an error in enrollment where the fingerprints were entered under another person's biographical information, the date of birth was transposed, or a possible legitimate name change on the subject, such as females that have since married.

The Department is also working to enhance biographic systems, such as the Arrival and Departure Information System (ADIS), and related interfaces across DHS components to increase interoperability, reduce processing errors, and improve data quality. A recent upgrade to the ADIS has improved the integration of US–VISIT biometric and biographic systems, and US–VISIT will continue to develop plans to improve identity resolution as funding permits.

*Question 2b.* What happens if an individual is found to have committed fraud by changing biographic information in order to enter into the United States? Are these individuals "flagged" in case of future travel?

Answer. If an individual is suspected of committing identity fraud, the subject is promoted to the IDENT watch list and a TECS lookout is created. Upon any future biometric and/or biographic screening, decision makers such as State Department Consular Officers, U.S. Citizenship and Immigration Services (USCIS) for benefits, and CBP Officers for admissibility will be notified of this suspected fraud. US–VISIT coordinates with the appropriate stakeholder for further action. If an individual who committed fraud was able to enter the United States, US–VISIT contacts ICE's National Security Investigations Division (NSID), Counterterrorism and Criminal Exploitation Unit or USCIS directly.

*Question 2c.* Does US–VISIT have plans to change its current identity resolution procedure in order to target individuals who may be attempting to defraud our travel system by entering the United States under multiple identities?

Answer. US–VISIT is reviewing the complete set of 825,000 records provided by the Inspector General to identify potential vulnerabilities and will coordinate with its partner agencies to improve the quality and accuracy of submitted data. A recent upgrade to the Arrival and Departure Information System has improved the integration of US–VISIT biometric and biographic systems, and US–VISIT will continue to develop plans to improve identity resolution in the event funding becomes available.

○