

**TEN YEARS AFTER 9/11: CAN TERRORISTS STILL  
EXPLOIT OUR VISA SYSTEM?**

---

---

**HEARING**  
BEFORE THE  
**SUBCOMMITTEE ON BORDER AND  
MARITIME SECURITY**  
OF THE  
**COMMITTEE ON HOMELAND SECURITY**  
**HOUSE OF REPRESENTATIVES**  
**ONE HUNDRED TWELFTH CONGRESS**  
FIRST SESSION

SEPTEMBER 13, 2011

---

**Serial No. 112-43**

---

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

72-930 PDF

WASHINGTON : 2012

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://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	BENNIE G. THOMPSON, Mississippi
DANIEL E. LUNGREN, California	LORETTA SANCHEZ, California
MIKE ROGERS, Alabama	SHEILA JACKSON LEE, Texas
MICHAEL T. MCCAUL, Texas	HENRY CUELLAR, Texas
GUS M. BILIRAKIS, Florida	YVETTE D. CLARKE, New York
PAUL C. BROUN, Georgia	LAURA RICHARDSON, California
CANDICE S. MILLER, Michigan	DANNY K. DAVIS, Illinois
TIM WALBERG, Michigan	BRIAN HIGGINS, New York
CHIP CRAVAACK, Minnesota	JACKIE SPEIER, California
JOE WALSH, Illinois	CEDRIC L. RICHMOND, Louisiana
PATRICK MEEHAN, Pennsylvania	HANSEN CLARKE, Michigan
BEN QUAYLE, Arizona	WILLIAM R. KEATING, Massachusetts
SCOTT RIGELL, Virginia	KATHLEEN C. HOCHUL, New York
BILLY LONG, Missouri	JANICE HAHN, California
JEFF DUNCAN, South Carolina	
TOM MARINO, Pennsylvania	
BLAKE FARENTHOLD, Texas	
MO BROOKS, Alabama	

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	HENRY CUELLAR, Texas
MICHAEL T. MCCAUL, Texas	LORETTA SANCHEZ, California
PAUL C. BROUN, Georgia	SHEILA JACKSON LEE, Texas
BEN QUAYLE, Arizona, <i>Vice Chair</i>	BRIAN HIGGINS, New York
SCOTT RIGELL, Virginia	HANSEN CLARKE, Michigan
JEFF DUNCAN, South Carolina	BENNIE G. THOMPSON, Mississippi ( <i>Ex Officio</i> )
PETER T. KING, New York ( <i>Ex Officio</i> )	

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 .....	5
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security .....	7
WITNESSES	
Mr. Thomas Winkowski, Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection, Department of Homeland Security:	
Oral Statement .....	10
Prepared Statement .....	11
Mr. Edward J. Ramotowski, Deputy Assistant Secretary, Acting, Bureau of Consular Affairs, U.S. Department of State:	
Oral Statement .....	14
Prepared Statement .....	16
Mr. John D. Cohen, Deputy Counter-Terrorism Coordinator, Department of Homeland Security:	
Oral Statement .....	24
Prepared Statement .....	25
Mr. Peter T. Edge, Deputy Associate Director, Homeland Security Investigations, Immigration and Customs Enforcement, Department of Homeland Security:	
Oral Statement .....	30
Prepared Statement .....	32
Mr. Richard M. Stana, Director, Homeland Security and Justice, Government Accountability Office:	
Oral Statement .....	36
Prepared Statement .....	38
APPENDIX	
The Honorable Henry Cuellar, a Representative in Congress From the State of Texas, and Ranking Member, Subcommittee on Border and Maritime Security:	
Slide .....	53



## TEN YEARS AFTER 9/11: CAN TERRORISTS STILL EXPLOIT OUR VISA SYSTEM?

Tuesday, September 13, 2011

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, McCaul, Quayle, Rigell, Duncan, Cuellar, Clarke, and Thompson (ex officio).

Also present: Representative Bilirakis.

Mrs. MILLER. I am going to call the hearing in order here this morning. Of course this is the Committee on Homeland Security, Subcommittee on Border and Maritime Security. I think we have a very interesting, interesting and critically important topic to discuss this morning. The title of our hearing is "Ten Years After 9/11: Can Terrorists Still Exploit Our Visa System?"

We will be hearing testimony from a fantastic distinguished panel whom I will be introducing in a moment. As I make my opening statement you may want to take a look at some of the pictures that we are going to have up on the screen of various terrorists, murderers, cowards, cockroaches, however you want to categorize these individuals that overstayed their visas.

So 2 days ago of course we commemorated the 10th anniversary of the devastating acts perpetrated by these cowardly terrorists who took the lives of nearly 3,000 of our fellow citizens. As a Nation most of us had not really heard before of al-Qaeda before that day despite their contributions which funded the 1993 attacks on the World Trade Center, fatwa that had declared war against our Nation in 1996, the bombing of our embassies in Kenya and Tanzania in 1998, and of course the bombing of the U.S.S. Cole in 2000. Despite these attacks we were really not prepared and certainly our countrymen paid a horrific price.

In Article I, Section 8 we find the enumerated powers of Congress, and in the first paragraph of that section you find what, in my opinion, is certainly the first and foremost responsibility of the Federal Government, and that is to provide for the common defense. The very purpose of this committee is aligned with this principal responsibility of the Government and to guard against another attack.

Photographs along our wall in this committee hearing room certainly remind us of our purpose to defeat al-Qaeda and like-minded

groups and to defend our homeland, which includes of course securing our borders.

On that day in September we learned a very hard lesson as a 9/11 Commission has noted. For terrorists, they said, travel documents are as important as weapons and four of the 9/11 hijackers had overstayed visas, a missed opportunity to prevent the attacks.

Since September 11, we have put a series of measures in place to strengthen our visa security process and today have a layered approach that begins overseas at the U.S. embassies and consulates around the world which pushes our border out to deter and prevent visa fraud and terrorists from obtaining travel documents. Immigration and Customs Enforcement agents and Customs and Border Protection officers are now stationed overseas to conduct additional background checks on prospective visa applicants. Certainly while this system is an improvement over what was in place before 9/11, it is by no means perfect. We will be exploring today what we can do to improve our system.

Our enemies are intent on attacking our country and are actively seeking to avoid our countermeasures. Our job is to be one step ahead instead of constantly reacting to their last attack.

In the case of the Christmas day bomber—I see his picture there—it certainly illustrates the lengths terrorists will go to thwart our security measures. The Christmas day bomber was known to the intelligence community. His father had approached the embassy in Nigeria with his concerns that his son may be involved in terrorism. But still he was able to fly on a valid U.S. visa. He tried to detonate his concealed explosive device 7 minutes before the plane was to land in Detroit. Of course I reside in the Detroit area, fly in and out of that airport, just flew out of it yesterday, which would have placed that plane certainly over my Congressional district, over southeast Michigan. So I am especially interested to hear from our witnesses today about the progress we have made to ensure that another known person of concern cannot board an aircraft with a valid U.S. visa.

Last week before the full committee, Ranking Member Cuellar and I were just talking, we heard from Representative Lee Hamilton and former Secretary Tom Ridge regarding the progress of the 9/11 Commission recommendations. The report recommended and Congress mandated a biometric exit program to ensure that foreign visitors have not overstayed their visa and have returned home. However, this administration has still not articulated the way forward on this vital program.

The U.S. Visitor and Immigration Status Indicator Technology, or US-VISIT as they call it, captures foreign nationals' fingerprints at the port of entry and at U.S. consulates overseas in instances where the individual is traveling on a visa. The fingerprints are then recorded and compared with fingerprints already in the Federal database to check for immigration violators, criminals, and others wanted for violation of U.S. laws.

In 2009, US-VISIT conducted an exit pilot project at the Detroit and Atlanta airports and generated 175 watch lists and more than 120 visa overstay hits. So I think if we are serious about controlling who comes into our Nation and preventing another attack, we need to get serious about an exit program. It has been more than

2 years since the pilot, and the Department again has yet to articulate a program or plan to move forward with a comprehensive exit plan in the air environment or elsewhere.

More than just preventing terrorists from entering the country, the lack of a visa exit program inhibits our ability to control our border. I think it is an interesting statistic that in this country as we talk about illegal immigrants and how many are here in our country, it is interesting to note that it is theorized that about 40 percent of everyone who is here illegally didn't come across the border. They are here because of overstay of visas, 40 percent. That is a very startling number.

Today there is a backlog of 757,000 unvetted visa overstay records. So we obviously have to do better than that, and I will be very interested as our hearing progresses about talking about this backlog, what we are doing to ensure that we don't have such a backlog in the future.

ICE pursues only a small fraction of these visa overstayers. By not seriously enforcing visa overstays, we are sending a message that if you make it past the port of entry, the chances of us ever finding you are slim to none. ICE enforcement memos put an additional question mark over our enforcement efforts there.

We do know that terrorists have a very strong affinity for using a student visa process to enter the country, as earlier this year a young man from Saudi Arabia purposely sought out a program that would allow him to come to the United States as a student. Then of course he has been accused of purchasing chemicals that he intended to use to construct an IED.

So we have a lot of questions about this, and certainly our visa security process needs to be robust. We have to deny terrorists the freedom of movement because 10 years ago we saw what failure looked like very unfortunately on that horrific day which we all commemorated just this past Sunday.

[The statement of Mrs. Miller follows:]

PREPARED STATEMENT OF CHAIRWOMAN CANDICE S. MILLER

SEPTEMBER 13, 2011

Two days ago we commemorated the 10th anniversary of the devastating acts perpetrated by cowardly terrorists who took the lives of nearly 3,000 of our fellow citizens.

As a Nation, most of us had not heard of al-Qaeda despite their financial contributions which funded the 1993 attacks on the World Trade Center, fatwa that declared war against our Nation in 1996, the bombing of our embassies in Kenya and Tanzania in 1998 and the bombing of the U.S.S. Cole in 2000. Despite these attacks, we were not prepared, and our countrymen paid the price.

In Article I Section 8, we find the enumerated powers of Congress, and in the first paragraph of that section you find what is, in my opinion, the principal responsibility of the Federal Government—to provide for the common defense.

The very purpose of this committee is aligned with the principal responsibility of the Government—to guard against another attack. Photographs along the wall here in the hearing room remind us of our purpose—to defeat al-Qaeda and like-minded groups and defend the homeland.

On that day in September, we learned a hard lesson—as the 9/11 Commission noted, “For terrorists, travel documents are as important as weapons.” Four of the 9/11 hijackers had overstayed visas—a missed opportunity to prevent the attacks.

Since September 11 we have put a series of measures in place to strengthen our visa security process. Today, we have a layered approach that begins overseas at U.S. Embassies and Consulates around the world which pushes our border out to deter and prevent visa fraud, and terrorists from obtaining travel documents.

Immigrations and Customs Enforcement agents and Customs and Border Protection officers are now stationed overseas to conduct additional background checks on prospective visa applicants.

While this system is an improvement over what was in place before September 11, it is by no means perfect.

Our enemies are intent on attacking our country, and are actively seeking to avoid our counter measures. Our job is to be one step ahead, instead of constantly reacting to their last attack.

The case of Umar Farouk Abdulmutallab illustrates the lengths terrorists will go to thwart our security measures.

The Christmas day bomber was known to the intelligence community, his father had approached the Embassy in Nigeria with his concerns that his son might be involved in terrorism, but he was able to fly on a valid U.S. visa.

Abdulmutallab tried to detonate his concealed explosive device 7 minutes before the plane was to land in Detroit—which would have placed that plane over my Congressional district. I am especially interested to hear from our witnesses about the progress we have made to ensure that another known person of concern cannot board an aircraft with a valid U.S. visa.

The 9/11 Commission report recommended and Congress mandated a biometric exit program to ensure that foreign visitors have not overstayed their visa and have returned home.

The U.S. Visitor and Immigrant Status Indicator Technology, or US-VISIT captures foreign nationals' fingerprints at the port of entry and at U.S. Consulates overseas in instances where the individual is traveling on a visa. The fingerprints are then recorded and compared with fingerprints already in Federal databases to check for immigration violators, criminals, and others wanted for violations of U.S. laws.

In 2009, US-VISIT conducted an exit pilot project at the Detroit and Atlanta airports and generated 175 watch list and more than 120 visa overstays hits. However, full deployment of an exit program is being delayed due to space and infrastructure constraints, and the remaining question of how to limit disruption to the flow of people and commerce into the United States. The Bipartisan Policy Center 9/11 Report Card lists this recommendation as "unfulfilled".

If we are serious about controlling who comes into the Nation and preventing another 9/11 attack, we need to get serious about an exit program. It has been more than 2 years since the pilot and the Department has yet to articulate a plan to move forward with a comprehensive exit plan in the air environment or elsewhere.

More than just preventing terrorists from entering the country, the lack of a visa exit program inhibits our ability to control the border. Nearly 40% of all illegal aliens do not sneak across the border in the dark of night; they walk through the front door, and never leave.

Today, there is a backlog of 757,000 unvetted visa overstay records. We can and must do better than that. I will be interested in hearing about our progress on this backlog and what we are doing to ensure that we do not have such a backlog in the future.

Immigration and Customs Enforcement pursues only a small fraction of these visa overstayers. By not seriously enforcing visa overstays, we are sending the message that if you make it past the port of entry, the chances of us ever finding you are slim to none.

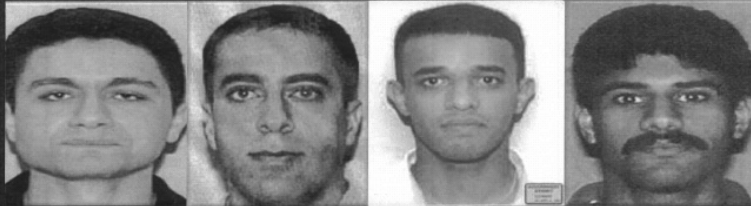
We know that terrorists have a strong affinity for using the student visa process to enter the country as earlier this year a young man from Saudi Arabia purposely sought out a program that would allow him to come to the United States as a student. He stands accused of purchasing chemicals he intended to use to construct an Improvised Explosive Device (IED).

I am sure my colleague, Mr. Bilirakis will have some questions for the witnesses on the status of our efforts in this area.

Our visa security process must be robust, and we must deny terrorists the freedom of movement because 10 years ago we saw what failure looked like.



## 9/11 Hijackers with Visa Violations



Mohammad  
Atta  
(Overstayed  
Tourist Visa)

Ziad Jarrah  
(Violated  
terms of  
Student Visa)

Satam al-  
Suqami  
(Overstayed  
Visa)

Nawaf al Hazmi  
(Overstayed  
Visa)

## Other High Profile Terrorist Visa Violators



Umar Farouk  
Abdulmutallab  
(Tourist Visa)

Zaccarias Moussaoui  
(Violated the terms of  
Student Visa)

Mahmud  
Abouhalima  
(Overstayed Tourist  
Visa)

Skeik Omar Abdel Rahman  
(Overstayed Visa)

Mrs. MILLER. At this time the Chairwoman would now recognize the Ranking Minority Member of the subcommittee, the gentleman from Texas, Mr. Cuellar, for his opening statement.

Mr. CUELLAR. Thank you, Chairwoman Miller, for holding this committee hearing. I also want to thank the Ranking Member of

the full committee for the work that he has done in the past on this issue. I am pleased that the subcommittee is meeting today to examine the issues of visa security, which is particularly appropriate as we recently marked the tenth anniversary of the terrorist attacks of September 11, 2001.

The 9/11 hijackers did not sneak into this country, did not cross a river, the Rio Grande, but rather entered the United States on visas. More recently the attempted bombing of an airline by Umar Farouk on Christmas day 2009 refocused attention on the vulnerabilities in the visa process.

Since 2001, the Department of Homeland Security and Department of State, with direction from Congress, have taken important steps to strengthen visa security, including efforts to identify and enforce overstays, individuals who are admitted to the United States legally either with or without a visa but then overstay their authorized period of admission. Of the approximately 11.5 million to 12 million unauthorized resident alien populations, the most recent estimates proposed that it is about 33 to 48 percent are overstays. That is almost 50 percent of all the people that got here, again I emphasize did not cross the Rio Grande but actually came in through a visa and overstayed.

Five of the 19 September 11, 2001 hijackers were overstays. There should be no argument against about the vital importance of the work completed by the Immigration and Customs Enforcement, ICE, and the Counterterrorism and Criminal Exploitation Unit, the CTCEU, whose primary responsibility is overstay enforcement.

In addition to the CTCEU overstay investigations, the primary responsibility for apprehending and removing overstays as well as aliens who did not have lawful immigration status rests with ICE, the Enforcement Removal Operation, the ERO. It is my understanding certain individuals subject to orders were removal from the United States are often delayed due to the respective host government relations with the United States and members.

Madam Chairwoman, I will have a handout on this, an overhead to go over this, and ask the witnesses on this particular issue. Consequently host countries refuse to accept the return of the nationals or use lengthy delay tactics. I know this is an issue that I sat down with John Morton in the State Department trying to get the State Department to move a little faster on this particular issue. I look forward to hearing more from the State and GAO about the U.S. former relations with these recalcitrant countries and why visas continue to be issued to individuals from such countries, and at what rate and as well as recommended steps for improvement and actions being taken. Again, Members, I would ask you to look at this particular issue as we talk about this.

Also within DHS and ICE, ICE has stood up a visa security unit, the VSUs, at high-risk visa issuing posts. It is my understanding, I might be wrong, but it is my understanding that historically there has been some tension between ICE and State regarding getting new VSUs established and hopefully we have gone beyond that turf battle. I hope to hear from the two agencies about whether they have made progress in overcoming those obstacles.

Customs and Border Protection also plays an important role in preventing terrorist travel to the United States. They have established the Immigration Advisory Program Units at key overseas airports to help screen travelers to the United States. Also I visited the CBP's National Targeting Center and I have seen the good work that they are doing along with their interagency partners, prescreening individuals en route to the country.

Many believe that given its security missions and resources DHS should play an even greater role in the visa processes. At a minimum we need to make most of our limited visa security resources and ensure that all agencies are doing their part.

I look forward to hearing from our DHS and State witnesses about how their agencies can work cooperatively to prevent those who would seek to do us harm from traveling to the United States.

It is worth noting that despite all the attention of the vulnerabilities along the Southern border, and again I emphasize to Members, an estimated 40 to 48 percent, as the Chairwoman said, of those currently in the United States illegally entered legally through the proverbial front door but have overstayed, again visas legally into the United States but overstayed, not crossing the Rio Grande.

We know that the overwhelming majority of those who enter the country do so for legitimate purposes. Even those who enter the country illegally or enter legally but overstay the majority mean this country no harm. But nevertheless those people have overstayed and violated the law.

However, a decade after 9/11 the fact remains that there are terrorists and others who seek to enter the United States for purposes to hurt us and our communities. So I look forward to a good, frank dialogue on this important Homeland Security matter, and I thank the Chairwoman Miller for holding this important hearing and the witnesses for joining us here today.

Thank you.

Mrs. MILLER. I thank the gentleman. Before I recognize the Ranking Member of the full committee I would ask unanimous consent that the gentleman from Florida, Mr. Bilirakis, who is the Chair of the committee's Subcommittee on Emergency Preparedness, Response, and Communications, be permitted to sit on the dais and participate in today's hearing.

Without objection, so ordered.

At this time the Chairwoman would recognize the Minority Ranking Member of the full committee, the gentleman from Mississippi, Mr. Thompson, for his opening statement.

Mr. THOMPSON. Thank you very much, Madam Chairwoman. I appreciate you holding this hearing. I also welcome our panel of witnesses.

In the aftermath of the September 11 attacks, Congress recognized the importance of securing the visa process and required it to be used as a counterterrorism tool. Since that time the Departments of Homeland Security and State have made important strides toward better securing the visa and passenger prescreening processes for travelers to the United States, efforts including establishing visa security units at high-risk embassies and consulates, deploying immigration advisory program personnel at foreign air-

ports and enhancing prescreening of airline passengers before they arrive in the United States. However, the attempted bombing of Northwest flight 253 on Christmas day 2009, by an individual with a valid U.S. visa served as a wake-up call about the persistent visa security vulnerabilities.

During the 111th Congress, the Committee on Homeland Security and this subcommittee held hearings to examine the circumstances surrounding the attempted Christmas day bombing. From our examination of the chain of events leading up to the incident, it is clear that there were several failures that allowed the perpetrator to board the U.S.-bound flight.

Today I look forward to hearing what progress has been made in closing those security gaps since that incident nearly 2 years ago. I also hope to hear that DHS and the State Department have taken proactive measures to address possible emerging threats to visa security. I have long held that we must develop a layered security approach that pushes borders out and begins the screening process far in advance of a passenger boarding a flight in this country.

Both DHS and the State Department have vital roles to play in this effort. Clearly defined responsibility and close coordination between the departments are essential to success. I want to hear from the witnesses today whether the turf battles between the departments are now a thing of the past or if they still linger. I certainly hope it is the former and not the latter.

Of course these security efforts require appropriate personnel and resources and that in turn requires adequate funding. Members of Congress who talk a good game on border security will need to put their money where their mouths are when it comes to funding these programs, even in tight budgetary times.

Just as we must ensure the security of the visa process for those entering the United States, we must also ensure individuals depart this country in a timely manner. As already indicated, over 40 percent of the persons unlawfully present in the United States enter this country legally and have overstayed. Among those millions of people may be a handful of those who seek to do us harm.

In accordance with the 9/11 Commission recommendations, Congress has repeatedly required DHS to deploy a biometric entry-exit system under US-VISIT to attract visitors to the United States. Yet a decade after September 11, 2001, we are no closer to having such a system than we were on that fateful day. Some of us read the paper this morning and I guess somebody is going to tell us something new about that in this hearing. I look forward to hearing that. The lack of progress toward this mandate under this administration and its predecessors is simply unacceptable. I hope to hear from our witnesses about how DHS can fully fulfill our 9/11 Commission recommendations and Congressional mandates. We will never truly have visa security until an entry-exit system is completed.

I thank the witnesses for being here today and I look forward to their testimony. I yield back.

Mrs. MILLER. I thank the gentleman for his comments. It is interesting to note that the administration is going to be making an announcement about this issue based on the fact that we are having a hearing about it. So I sometimes think it is exactly what Con-

gress needs to be doing, exercising its oversight responsibilities to get some action on various things.

What I will do is go through and read the bios of our very distinguished panel, and we appreciate you all coming. We can go through rather than interrupting each time.

First Mr. Thomas Winkowski, who is the Assistant Commissioner from the Office of Field Operations, U.S. Customs and Border Protection, Department of Homeland Security, was appointed the Assistant Commissioner in August 2007. He is responsible for operations at 20 major field offices, 331 ports of entry, 58 operational container security initiative ports, and 15 preclearance stations in Canada, Ireland, the Caribbean. Previously he served as Director of Field Operations in Miami, where he was responsible for managing all inspectional operations at the Miami International Airport and the seaport, Port Everglades, Fort Lauderdale International Airport, and West Palm Beach and Key West as well.

Then we will hear from Mr. Edward Ramotowski, who is the Deputy Assistant Secretary, Acting, Bureau of Consular Affairs, the U.S. Department of State. He assumed his current position as Managing Director of Visa Services at the U.S. Department of State in August 2009, and in that position he oversees the visa office in Washington, DC, two domestic processing centers, as well as visa operations at over 200 U.S. embassies and consulates abroad. From August 2006 to July 2009 he served as principal officer at the U.S. Consulate General in Guadalajara, Mexico. He has previously worked as a Special Assistant to the Assistant Secretary of State for Consular Affairs, Chief of the Consular Section of the U.S. Embassy in Nassau, Bahamas and the U.S. Council in Warsaw, Poland.

Then we will hear from Mr. John Cohen, who is the Deputy Counterterrorism Coordinator, Department of Homeland Security. He serves as the Principal Deputy Coordinator for Counterterrorism at the U.S. Department of Homeland Security, and as the Senior Advisor on Counterterrorism, Law Enforcement and Information Sharing. He has also served as the Senior Advisor to the Program Manager for the Information Sharing Environment, Office of the Director of National Intel, where he authored and coordinated the implementation of key components of the National Strategy for Information Sharing.

Peter Edge, the Deputy Associate Director, Homeland Security Investigations, Immigration and Customs Enforcement, Department of Homeland Security, began his law enforcement career in 1986 in Essex County, New Jersey Prosecutor's Office, prior to his selection as a Special Agent was with the U.S. Customs Service in Newark, New Jersey. In 2005, Mr. Edge was promoted to the position of Assistant Special Agent in Charge of the SAC New York office where he lead high-profile investigative components such as the El Dorado Task Force, the New York High Intensity Financial Crime Area, JFK International Airport, and the Immigration Division. Today he serves as the Deputy Associate Director of Homeland Security Investigations for the U.S. Immigration And Customs Enforcement.

Then we will hear from Mr. Richard Stana, we welcome him back to the committee again, the Director of the Homeland Security

and Justice, Government Accountability Office. During his 27-year career with the GAO, he has directed reviews on a wide variety of complex domestic and military issues while serving in headquarters, field, and overseas offices. Most recently he has directed GAO's work relating to immigration, customs law enforcement, drug control corrections, court administration, and election system.

So you can see we have a very, very distinguished panel. We will begin with Mr. Winkowski. The floor is yours, sir, for your prepared testimony.

**STATEMENT OF THOMAS WINKOWSKI, ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION, DEPARTMENT OF HOMELAND SECURITY**

Mr. WINKOWSKI. Good morning, Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee. Thank you for the opportunity to appear today to discuss CBP's visa security efforts.

Since its establishment in 2001, the National Targeting Center's priority mission has been to provide tactical targeting and analytical research support for CBP's antiterrorism efforts. The NTC develops tactical data and actual intelligence to prevent high-risk travelers and goods from entering the United States.

Centralized NTC targeting endeavors combined with interagency collaboration as well as robust partnerships with our foreign counterparts ensure a coordinated response to terrorists in National security events.

CBP works in coordination and collaboration with a number of Government agencies with broad authorities, robust capabilities, and missions that are complimentary for other Nation's security. Each agency's unique capability and resources leverage DHS's layered risk management approach to safeguarding U.S. borders.

A few critical examples of this, Chairwoman Miller, the NTC coordinates with the terrorist screening center to resolve every terrorist screening database encounter. We work closely with the State Department to enhance visa security. As a result, the State Department has revoked more than 1,000 visas based on CBP's vetting results and recommendations.

ICE has collocated visa security personnel at the National Targeting Center to augment and expand current operations. We are collaborating with TSA in the private sector on an air cargo advanced screening pilot which was implemented following the October 2010 attempts by extremists to ship explosive devices in their cargo shipments.

Additionally, CBP has information-sharing agreements with foreign partners, including Canada, the United Kingdom, New Zealand, and Australia.

On an average day CBP processes nearly 1 million travelers at our ports of entry. The challenge faced by CBP each day is rapidly and accurately identifying those individuals that pose a threat to the United States and prevent their entry into the country. CBP takes action at a number of points in the travel continuum.

In the area of visa and visa waiver program security, while the State Department is responsible for visa issuance, CBP has

partnered with the State Department to ensure the visa issuance and travel process. In March 2010 we implemented a system that vets all visas on a continuous basis.

Under the Visa Waiver Program and the Electronic System for Travel Authorization, ESTA, we conduct enhanced vetting on Visa Waiver Program applicants in advance of travel. As you recall, that was a 9/11 Commission recommendation.

In the area of predeparture screening, CBP now conducts predeparture screening of all travelers prior to boarding flights bound for the United States. When the NTC identifies a high-risk traveler through this process, we coordinate with our immigration advisory program offices that are located in 8 airports around the world or our regional carry liaison group which is located in three areas in the United States, in Honolulu, JFK Airport, and Miami International Airport, to resolve the issues or recommend to the carrier that a traveler not be boarded.

Now as a result of these efforts 100 percent of travelers on all flights arriving at and departing from the United States are checked against Government databases prior to boarding a flight. In fiscal year 2011, CBP made more than 2,000 no-board recommendations to carriers. In the area of outbound in addition to predeparture screening of inbound travelers, we have also enhanced our outbound screening efforts. As a result CBP has notable success in identifying and preventing the departure of the Time Square bomber in May 2010 as well as a suspected serial killer that was departing Atlanta airport in August 2010.

In closing, CBP is continuing proactively looking for solutions to threats to the homeland identified by operationalizing intelligence through real-time targeting, officer screening, and data sharing. Partnering with our agencies and nations, effectively extending our borders and exchanging information, makes this a truly global fight against terror.

Our future state should include additional screening processes and methods to make this protection a greater reality so the American public remains safe. Chairwoman Miller, Ranking Member Cuellar, and Members of the subcommittee thank you for the opportunity to testify. I look forward to answering your questions.

[The statement of Mr. Winkowski follows:]

PREPARED STATEMENT OF THOMAS WINKOWSKI

SEPTEMBER 13, 2011

Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee, thank you for the opportunity to appear today to discuss the good work of U.S. Customs and Border Protection (CBP) related to ensuring and enforcing security measures implemented since the attacks of September 11, 2001. I appreciate the committee's leadership and your commitment to helping ensure the security of the American people.

CBP'S ROLE IN MULTIPLE LAYERS OF DEFENSE

CBP and, more broadly, Department of Homeland Security (DHS) continually refine our risk-based and layered approach to security, focusing our resources on the greatest vulnerabilities, extending our borders outward, and interdicting threats before they reach the United States. DHS, in cooperation with our interagency and foreign partners, is now screening people and goods earlier in the travel process. With more advanced and better quality data than ever before, we now employ an

extensive network of research and analysis well before a traveler applies for admission at a U.S. port of entry.

Depending on the traveler's point of origin and travel and entry document requirements, the screening process can begin in a number of ways: With the application for a visa, application for electronic travel authorization, purchase of an airline ticket, or arrival at a foreign airport or domestic port of entry. At each step along the way, CBP, in cooperation with other Government agencies and commercial carriers, reviews information about the traveler, including their documents, their effects, and/or their responses to questions, prior to arrival at a U.S. port of entry. Several Federal agencies are responsible for different aspects of our aviation security, while other countries and the private sector—particularly the air carriers—also have important roles to play. These multiple layers of defense across departments and agencies secure the aviation sector and ensure the safety of the traveling public.

The foiled plot to bring liquid explosives onboard U.S.-bound flights from the United Kingdom in 2006, the attempted bombing of Northwest Flight 253 on December 25, 2009, the failed Times Square bombing in May 2010, and the attempts to mail explosive devices within printer cartridges from Yemen in October 2010 are all powerful illustrations that terrorists continue to try to overcome security measures we have enacted since September 11, 2001.

CBP continually evaluates and supplements existing security measures with additional enhancements to strengthen our ability to identify and prevent the international travel of mala fide travelers and cargo. The success of these additional security measures depends in great part on our ability to gather, share, and respond to information in a timely manner—using both strategic intelligence to identify existing and emerging threat streams, and tactical intelligence to perform link analysis and targeted responses.

#### *CBP and Intelligence*

As part of our efforts to screen passengers bound for the United States, CBP uses the U.S. Government's consolidated terrorist watch list, specifically, the Terrorist Screening Database (TSDB), managed by the Terrorist Screening Center. In addition, we use additional relevant information from the intelligence community to determine whether someone may be a risk to a flight, requires further screening and investigation, should not be admitted, or should be referred to appropriate law enforcement personnel.

Further, CBP's Office of Intelligence and Investigative Liaison (OIIL), which serves as the situational awareness hub for CBP, provides timely and relevant information along with actionable intelligence to operators and decision-makers and improving coordination of CBP-wide operations. Through prioritization and mitigation of emerging threats, risks, and vulnerabilities, OIIL helps CBP to better function as an intelligence-driven operational organization and turns numerous data points and intelligence into actionable information for CBP officers and analysts.

#### *National Targeting Center*

The National Targeting Center (NTC) is another key tool for DHS in analyzing, assessing, and making determinations based on the TSDB and other intelligence information. The NTC is a 24/7 operation, established to provide tactical targeting information aimed at interdicting terrorists, criminal actors, and contraband at the earliest point. CBP's Automated Targeting System (ATS) is a decision-support tool crucial to the operation of the NTC and is a primary platform used by DHS to match travelers, conveyances, and shipments against law enforcement information and known patterns of illicit activity.

#### *Safeguards for Visas and Travel*

One of the initial layers of defense in securing air travel is preventing dangerous persons from obtaining visas, travel authorizations, and boarding passes. Before boarding a flight destined for the United States or arriving at a U.S. port of entry, most foreign nationals need to obtain a visa—issued by a U.S. embassy or consulate—or, if they are eligible to travel under the Visa Waiver Program (VWP), they must apply for a travel authorization issued through the Electronic System for Travel Authorization (ESTA).<sup>1</sup>

The Department of State (DOS) is responsible for visa issuance. DOS also screens all visa applicants' biographic data against the DOS Consular Lookout and Support System, which includes entries that alert consular officers to the existence of TSDB

<sup>1</sup>Exceptions would be citizens of countries under other visa exempt authority, such as Canada. Citizens of countries under visa exempt authority entering the U.S. via air are subjected to CBP's screening and inspection processes prior to departure. In the land environment, they are subjected to CBP processing upon arrival at a U.S. port of entry.



files, for records related to potential visa ineligibilities and checks their biometric data (i.e., fingerprints and facial images) against other U.S. Government databases for records indicating potential security, criminal, and immigration violations prior to the issuance of the visa. For individuals traveling under the VWP, CBP operates ESTA, a web-based system through which individuals must apply for travel authorization prior to traveling to the United States. Through ESTA, CBP conducts enhanced vetting of VWP applicants in advance of travel to the United States in order to assess whether they could pose a risk to the United States or the public at large. Additionally, through interactive communications with CBP, air carriers are required to verify that VWP travelers have a valid authorization before boarding an aircraft bound for the United States.

#### *Pre-departure Vetting*

CBP can also gather information and assess risk at the point of travel booking. CBP conducts pre-departure and outbound screening for all international flights arriving into and departing from the United States. This works in concert with the Transportation Security Administration's Secure Flight program, which vets 100 percent of passengers flying to, from, and within the United States against the No Fly and Selectee portions of the known or suspected terrorist watch list, or TSDB. The NTC uses a variety of data sources and automated enforcement tools to perform its function. The process starts when a traveler purchases a ticket for travel to the United States; a Passenger Name Record (PNR) may be generated in the airline's reservation system. PNR data contains various elements, including information on itinerary, co-travelers, changes to the reservation, and payment information. CBP receives PNR data from the airline at various intervals beginning 72 hours prior to departure and concluding at the scheduled departure time.

CBP uses the Automated Targeting System (ATS) to then evaluate the PNR data against "targeting rules" that are based on law enforcement data, intelligence information, and past case experience. ATS allows CBP to identify and interdict travelers with potential nexus to transnational crime, including terrorism, narcotics trafficking, and human smuggling.

The traveler's check-in provides the next opportunity in the travel process for CBP to gather information and assess risk. On the day of departure, when an individual checks in for his or her intended flight, the basic biographic information from the individual's passport is collected by the air carrier and submitted to CBP's Advance Passenger Information System (APIS). Carriers are required to verify the APIS against the traveler's government-issued travel document and provide the data to DHS at least 30 minutes before departure, or up to the time of securing the doors if using APIS Quick Query, for all passengers and crew on board.<sup>2</sup> APIS data contains important identifying information that is not included in PNR data, including verified identity and travel document information such as a traveler's date of birth, citizenship, and travel document number. DHS vets APIS information on all international flights to and from the United States against the TSDB, as well as against criminal history information, records of lost or stolen passports, public health records, and prior immigration or customs violations and visa refusals. APIS is also connected to Interpol's lost and stolen travel document database for routine queries on all foreign passports used for check-in.

Another layer in the vetting process is the Immigration Advisory Program (IAP), which stations CBP officers at eight foreign airports in six countries in coordination with the host foreign governments. Officers are deployed to these key transit hubs and work with border control authorities, foreign law enforcement agencies, and air carriers to identify known or suspected terrorists and other high-risk travelers and assist in preventing them from boarding aircraft destined for the United States. CBP officials at the NTC support IAP by screening all travelers against the TSDB, including the subset No Fly list, ESTA denials, visa revocations, public health look-outs, lost and stolen passport records, and all State Department records for persons identified as actually, or likely, having engaged in terrorist activity. At IAP locations, CBP officers can make "no board" recommendations to carriers and host governments regarding passengers bound for the United States who may constitute security risks, but officers do not have the authority to arrest, detain, search, or prevent passengers from boarding planes. Those authorities lie with the host government.

After the attempted bombing on December 25, 2009, CBP expanded on the NTC's IAP pre-departure screening efforts to include screening at all foreign airports with direct flights departing to the United States to identify and assess risks prior to

<sup>2</sup> APIS is the electronic data interchange for air carrier transmissions of electronic passenger, crew member, and non-crew member manifest data.

travel and prevent the boarding of high-risk travelers. When pre-departure screening identifies a potential high-risk traveler, the NTC confirms the information through vetting procedures, and then coordinates the issuance of “no board” recommendations to carriers via the nearest ICE or CBP Attaché, Air Carrier Security Office, and the CBP Regional Carrier Liaison Group. Now, as a result of these efforts, 100 percent of travelers on all flights arriving at and departing from the United States are checked against Government databases prior to boarding a flight. During fiscal year 2011 to date, pre-departure screening by the NTC has kept more than 2,000 high-risk or otherwise inadmissible travelers from boarding flights destined for the United States.

In March 2010, the NTC implemented a new program to conduct continuous vetting of U.S. nonimmigrant visas that have been recently issued, revoked, and/or denied. The continuous vetting ensures that changes in a traveler’s visa status are identified in near real-time, allowing CBP to immediately determine whether to provide a “no board” recommendation to a carrier or recommend that DOS revoke the visa, or whether additional notification should take place for individuals determined to be within the United States. If a violation is discovered, and the person is scheduled to travel to the United States, CBP will request that DOS revoke the visa and recommend that the airline not board the passenger. If no imminent travel is identified, and derogatory information exists that would render a subject inadmissible, CBP will coordinate with DOS for a prudential visa revocation. If the subject of an existing visa revocation initiated by the DOS or recommended by CBP is found to be in the United States, CBP will notify the ICE Counterterrorism and Criminal Exploitation Enforcement Unit for further action as appropriate.

Additionally, ICE has co-located Visa Security Program (VSP) personnel at the NTC to augment and expand current operations. ICE special agents and intelligence analysts conduct thorough analysis and in-depth investigations of high-risk visa applicants. The focus of the VSP and NTC are complementary: The VSP is focused on identifying terrorists and criminal suspects and preventing them from exploiting the visa process and reaching the United States, while the NTC provides tactical targeting and analytical research in support of preventing terrorist and terrorist weapons from entering the United States. The co-location of VSP personnel at the NTC has helped increase both communication and information sharing.

*Vetting While En Route to the United States and Upon Arrival*

While flights are en route to the United States, CBP continues to evaluate the updated APIS and PNR information submitted by the airlines. Based on the information garnered during the in-flight analysis, as well as the CBP officer’s observations at the port of entry, a determination is made as to whether the traveler should be admitted to the United States following primary inspection or referred for a secondary inspection.

CONCLUSION

As this committee no doubt knows, we live in a world of ever-evolving risks, and we must move as deftly as possible to identify and fix security gaps and to anticipate future vulnerabilities. CBP will continue to work with our colleagues within DHS, and with DOS, and the intelligence community to address these challenges.

Chairwoman Miller, Ranking Member Cuellar, and Members of the subcommittee, thank you for this opportunity to testify. I look forward to answering your questions.

Mrs. MILLER. Thank you very much. The Chairwoman now recognizes Mr. Ramotowski for his comments and his testimony.

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

Mr. RAMOTOWSKI. Good morning, Madam Chairwoman, Ranking Member Cuellar, and distinguished Members of the subcommittee. As a 25-year veteran of the United States Foreign Service, it is an honor to testify before you just 2 days after our Nation marked such a somber event, the 10-year anniversary of the 9/11 attacks. My colleagues and I in the Foreign Service in the State Department will never forget that day, and we are fully determined to ensure that such a tragedy does not occur again.

My focus today is on how the Department of State reformed the visa process in the 10 years since 9/11 to eliminate loopholes for terrorists to exploit our system, as well as additional measures the Department undertook in response to the December 25, 2009 attempted airline bombing.

Today visa processing rests on a multi-layered approach to security, what we refer to as the five pillars, technological advances, biometric innovations, personal interviews, interagency data sharing, and intensive training. All of these pillars supported the Department's response to the Christmas day incident and we are continually refining and improving them to deal with constantly evolving threat.

Among the key measures taken, we improved our visa Viper terrorist information reporting program, by directing all chiefs of mission to ensure that it was working effectively at all their posts and instructing consular officers to include complete information about the U.S. visa status of any individuals included in Viper reporting.

As a second critical step, we issued new instructions to officers on visa revocation procedures, and we enforced standing guidance on their discretionary authority to deny visas under Section 214(b) of the Immigration and Nationality Act with specific reference to cases that raise security and other serious concerns.

We also created a dedicated revocation unit in Washington that is focused exclusively on ensuring that any derogatory information on a U.S. visa holder is rapidly evaluated and acted upon.

As another step, we improved the capability of consular systems to match visa records against new and emerging derogatory information, to support the revocation process in appropriate cases. We employ sophisticated name searching algorithms to ensure matches to derogatory information contained in the millions of records in our lookout system. We use our authority to immediately revoke a visa in circumstances where we believe there is an imminent threat.

The continuous vetting of the database of issued visas by the Department and our partner agencies helps ensure that new derogatory information that arises after visa issuance is rapidly analyzed for revocation purposes.

Let me briefly turn to the overall visa security and the five-pillar system we have in place today. Before any visa is issued the applicant's fingerprints are screened against DHS and FBI databases. We use facial recognition technology to screen visa applicants against a watch list of photos obtained from the terrorist screening center as well as visa applicant photos contained in our own consular consolidated database.

Our new on-line visa application forms have the potential to provide consular and fraud prevention officers as well as our intelligence and law enforcement partners the opportunity to analyze data in advance of a visa interview, including the detection of potential nonbiographic links to derogatory information. We have ambitious plans to screen more of this data with our partner agencies to make the visa system even more secure.

We also invest heavily in our people. Each consular officer completes the basic consular course and receives continuing advanced education in interviewing and name-checking techniques through-

out his or her career. Language fluency and area and culture knowledge are other important skill sets that consular officers use daily to improve the adjudication of visas.

We work closely with our partners to ensure that no terrorist receives a visa or is admitted into our country. Our vast database of visa information is fully available to other agencies and we have specifically designed our systems to facilitate comprehensive data sharing. In return we have unprecedented levels of cooperation with law enforcement and intelligence agencies and benefit from their capabilities and resources in ways that were not possible at the time of 9/11 or even on Christmas day 2009.

Distinguished Members of the committee, our current layered approach to border security screening in which each agency applies its particular strengths and expertise best serves our border security agenda while furthering traditional U.S. interest in legitimate travel, trade promotion, and exchange of ideas. The United States must meet both goals to guarantee our long-term security.

Thank you and I welcome your questions.

[The statement of Mr. Ramotowski follows:]

PREPARED STATEMENT OF EDWARD J. RAMOTOWSKI

SEPTEMBER 13, 2011

Good afternoon Madame Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the committee. I thank you for this opportunity to update you on the steps we have taken to increase the security of the visa process.

The Department of State (the "Department") is dedicated to the protection of our borders, and has no higher priority than the safety of our fellow citizens. We are the first line of defense in border security because the Department is often the first Government agency to have contact with foreign nationals wishing to visit the United States. We are committed, along with our partner agencies, to a layered approach to border security that will enable 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.

CORRECTIVE ACTIONS IMPLEMENTED AFTER DECEMBER 25, 2009

After the December 25, 2009 attempted terrorist attack on Northwest flight 253, the President ordered corrective steps to address identified weaknesses in the systems and procedures we use to protect the people of the United States. In the months following the attack, we reviewed our requirements for reporting potential terrorists who are not applying for visas, which fall under our "Visas Viper" program, as well as visa issuance and revocation criteria, and we introduced technological and procedural enhancements to facilitate and strengthen visa-related business processes.

Our immediate focus was on the deficiencies identified following the attempted attack on flight 253 by Umar Farouk Abdulmutallab. On the day following his father's November 2009 visit to the U.S. Embassy in Abuja, Nigeria, the Embassy sent a Visas Viper cable to the Department and the Washington intelligence and law enforcement community, stating that Abdulmutallab may be involved with Yemeni-based extremists. In sending the cable and checking State Department records to determine whether Abdulmutallab had a visa, Embassy officials misspelled his name, and as a result of that misspelling, information about previous visas issued to him, and the fact that he held a valid U.S. visa, was not included in the cable.

At the same time, the Consular Section entered Abdulmutallab's name into the Consular Lookout and Support System (CLASS), our on-line database of lookout information. This correctly spelled CLASS lookout was shared automatically with the primary lookout system used by the Department of Homeland Security (DHS) and accessible to other agencies. On the basis of this CLASS entry, DHS's U.S. Customs and Border Protection (CBP) determined, after the flight departed Amsterdam, that Abdulmutallab warranted secondary screening upon arrival in Detroit. Additional reporting on this case carried the correct spelling, with additional reports reaching the necessary agencies in Washington.

To address the deficiencies identified in that review, including our concerns with the Visas Viper process, we took immediate action to improve the procedures and content requirements for Visas Viper cable reporting. We directed all Chiefs of Mission to ensure that the Visas Viper program functioned effectively at their posts, and that all appropriate agencies and offices at post contributed relevant information for Viper nominations. We instructed consular officers to include complete information about all previous and current U.S. visas in Visas Viper cables. The guidance cable included specific instructions on methods to comprehensively and intensively search the database of visa records so that all pertinent information is obtained. We also issued new instructions to officers 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 Immigration and Nationality Act (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 officer training for several years.

In addition to changes in standard procedures for searching visa records, we immediately began working to refine the capability of our current systems, with a particular focus on matching records of currently valid visas against new and emerging derogatory information, to support visa revocation in appropriate cases. For visa applications, we employ strong, sophisticated name-searching algorithms to ensure matches between names of visa applicants and any derogatory information contained in the 42 million records found in CLASS. This robust searching capability, which takes into account variations in spelling, has been central to our procedures since automated lookout system checks were mandated following the 1993 World Trade Center bombing. We constantly use our significant and evolving experience with searching mechanisms for derogatory information to improve the systems for checking our visa issuance records.

CLASS has grown more than 400 percent since 2001—largely as a result of improved data sharing 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 the intelligence community. CLASS also includes unclassified records regarding known or suspected terrorists (KSTs) from the Terrorist Screening Database, which is maintained by the Terrorist Screening Center (TSC) and contains unclassified data on KSTs nominated by all U.S. Government sources. We automatically run all applicants' names against the Department's Consular Consolidated Database (CCD), which holds our historical visa records, as part of our on-going commitment to optimizing the use of our systems to detect and respond to derogatory information regarding visa applicants and visa holders. 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.

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 has a U.S. visa.

Cases for revocation consideration are forwarded to the Department by our consular offices overseas, CBP's National Targeting Center (NTC), and other 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, as well as to biometric identity systems, and then shared in near-real time (within about 15 minutes) with the DHS lookout systems used for border screening. As part of its enhanced "Pre-Departure" initiative, CBP uses these VRVK records, among other lookout codes, to recommend that airlines should not board certain passengers on flights bound for the United States. Almost every day, we receive requests to review and, if warranted, revoke any outstanding visas for 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, and thus prevent 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 ap-

proximately 60,000 visas for a variety of reasons, including nearly 5,000 for suspected links to terrorism; 1,451 of those occurring since the attempted attack on December 25, 2009. Following that incident, we reviewed the last 10 years of Visas Viper nominations, as well as “P3B” entries (potentially ineligible for a visa due to suspected ties to terrorism) in CLASS to determine whether Visas Viper subjects were properly watch listed, and to determine the visa status of all P3B subjects. The Department’s Visa Office completed a review of all 2001–2010 data and revoked 30 visas.

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.

#### A MORE SECURE VISA APPLICATION PROCESS

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 DHS’s Automated Biometric Identification System (IDENT), which has a watch list containing available fingerprints of terrorists, wanted persons, and immigration law violators; and against the FBI’s 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 2010, IAFIS returned more than 57,000 criminal arrest records to posts. The Biometric Visa Program partners with the DHS US–VISIT Program to enable CBP officers at ports of entry to match the fingerprints of persons entering the United States with the fingerprints that were taken during visa interviews at overseas posts and transmitted electronically to DHS IDENT. This biometric identity verification at ports of entry has greatly enhanced CBP officers’ ability to identify photo-substituted visas and the use of valid visas by imposters.

We also use facial recognition technology to screen visa applicants against a watch list of photos of known and suspected terrorists obtained from the FBI’s TSC, as well as the entire gallery of visa applicant photos contained in our CCD. Facial recognition screening has proven to be another effective way to combat identity fraud.

The Consular Electronic Application Center (CEAC) is another major technological advance. CEAC is an electronic platform where applicants submit visa applications and photos via the internet, eliminating paperwork, decreasing visa application and adjudication times, and reducing the number of forms applicants must complete. The worldwide roll out of the on-line DS–160 nonimmigrant visa application form is complete, and we are currently piloting the on-line DS–260 immigrant visa application form. These new on-line forms provide consular and fraud officers the opportunity to analyze data in advance of the interview, enhancing their ability to make decisions, and soon will afford intelligence and law enforcement agencies opportunities to analyze visa application data before applicants appear for their interviews. The on-line forms offer foreign language support; however, applicants are required to answer in English, to facilitate information sharing between the Department and other Government agencies. The new application forms are “smart,” meaning that certain answers to questions will trigger subsequent questions. The system will not accept applications if the security-related questions have not been fully answered, and “irregular” answers are flagged to ensure that consular officers address them in the interview.

In April 2011, we greatly enhanced the way we track visa fraud. We globally deployed a tool called the Enterprise Case Assessment Service that provides a platform to store fraud-related research that used to be stored outside of consular systems. This new tool associates fraud-related information with visa records, making it available to consular officials around the world. Should fraud be confirmed during the course of a visa interview, consular officers can record that data in this new tool, where it can be easily referenced if the individual attempts to 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. We hope soon to be able to share this new data source with our U.S. Government partners to enhance interagency cooperation on fraud prevention.

## STUDENT AND EXCHANGE VISITOR VISAS

I am aware that the Members of this committee have a keen interest in the processing of student and exchange visitor visas. Consular processing of these visa classes follows the same sequence of clearances as the other visa classifications, including collection of biometrics and submission of the on-line DS-160 form. All CLASS and other security checks apply.

In addition, in order for an applicant to demonstrate that he/she is qualified to apply for a student or exchange visitor visa, the applicant must have been issued specific documentation, in addition to what is required for other visas classes, and present it to the consular officer at the time of interview. A student, for instance, must have been issued a Form I-20A-B by the school he/she will attend in order to apply for an F-1 student visa (or for dependants, an F-2 visa), or a Form I-20M-N if the student has been accepted at a vocational school. In order to qualify for an exchange visitor visa (J-1, dependent J-2), the applicant must present a Form DS-2019 issued by the designated sponsor of one of the 15 categories of exchange visitor programs.

Upon acceptance to the chosen educational institution or organization, the student or exchange visitor is assigned a unique ID number in the Student and Exchange Visitor Information System (SEVIS), a DHS database. The individual retains the same number throughout his or her educational career.

For an applicant to be found eligible for an F, M, or J visa, the student must meet the requirements specific to student or exchange visitor status (accepted at a school authorized by DHS to issue the Form I-20, pursuing a degree or certificate with sufficient finances, etc.) necessary to participate in the type of program chosen. In addition, the student must demonstrate the intent to engage only in approved activities for the visa class, the ability to meet the financial requirements of the activity undertaken, and demonstrate a present intent to depart the United States upon the completion of the chosen activity.

## TRAINING

Consular officers are trained to take all necessary steps during the course of making a decision on a visa application to protect the United States and its citizens. Every consular officer is required to complete the Department's Basic Consular Course at the National Foreign Affairs Training Center prior to performing consular duties. The course places strong emphasis on border security, featuring in-depth interviewing and name-checking technique training, as well as fraud prevention. Throughout their careers, consular officers receive continuing education in all of these disciplines to ensure they integrate the latest regulations and technologies into their adjudicatory decisions.

To augment this training and strengthen the security of the visa program, in early 2010 the Department launched a program to provide consular officers overseas with enhanced security clearances. This allows them to participate more fully in posts' review of security issues that bear on the issuance of passports and visas, and the protection of U.S. citizens traveling and living abroad. In the past few months, a concerted push on this project resulted in the tripling of the number of highly-cleared consular officers (to more than 150) in key positions at high-threat posts. The Office of Counterintelligence and Consular Support, in the Bureau of Intelligence and Research, has increased its efforts to identify relevant reporting for review by those consular officers.

## SECURITY ADVISORY OPINIONS

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 ineligibilities. Consular officers receive extensive training on the SAO process, including modules on cultural and religious naming conventions, which assists them in identifying applicants who require additional Washington vetting. The SAO process requires the consular officer to suspend visa processing pending interagency review of the case and additional guidance. Most SAOs are triggered by clear and objective circumstances, such as nationality, place of birth, residence, or visa name check results. 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 INA.

## THE VISA SECURITY PROGRAM

The Department of State believes that the Visa Security Program (VSP), under which DHS deploys U.S. Immigration and Customs Enforcement (ICE) special agents to conduct visa security screening and investigations at certain overseas consular posts, is a valuable component of the U.S. Government's overall policy of protecting our borders. 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, as well a number of data-sharing arrangements.

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 Visa Security Units provide timely and valuable on-site vetting of visa applications and other law enforcement support to our consular officers. We work very closely with DHS to ensure that no terrorist receives a visa or is admitted into our country.

Reports from our posts with ICE visa security operations suggest that, as the VSP has matured over the past few years, ICE special agents have, where resources permit, moved beyond a singular focus on visa application review. They have been able to contribute their expertise and resources to enhance our response to all kinds of threats to the visa and immigration processes—terrorism, human smuggling and trafficking, and trafficking in a wide variety of contraband. As reported by one of our missions, "(i)n addition to their concerns with visa security, [ICE special agents'] efforts have also led to arrests and indictments in the areas of child pornography and countering the proliferation of controlled technology. This is a win-win partnership."

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 special agents in Washington review our visa databases and advise posts of emerging information about visa holders. Another important aspect of our Washington partnership is the resolution of issues raised as the VSP expands to more posts. In January 2011, the Department's Bureaus of Consular Affairs (CA) and Diplomatic Security (DS) concluded a Memorandum of Understanding (MOU) with ICE. This MOU governs VSP-Department of State interactions within visa sections, procedures for resolving the very few disputed visa cases that emerge from the VSP review process, and collaboration between ICE special agents and their DS law enforcement colleagues assigned as Regional Security Officers (RSOs) or Assistant Regional Security Officer Investigators (ARSO-Is) assigned to consular sections.

Under the umbrella of section 428 of the Homeland Security Act and the implementing Memorandum of Understanding between the Departments of State and Homeland Security, we work together to resolve cases. When warranted, DHS special agents assigned to the VSP 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 with DHS to ensure that terrorists do not receive visas and to expeditiously revoke visas as appropriate.

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.

Currently, there are 19 visa-issuing posts in 15 countries with an ICE VSP presence. Before submitting an NSDD-38 request, ICE officials, with the support of senior State 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 VSP.

## LAYERED SECURITY AND DATA SHARING

The Department embraces a layered approach to security screening. In addition to our support of the VSP, over the past 7 years the Department and DHS have increased resources significantly, improved procedures, and upgraded systems devoted to supporting the visa function. 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 fin-



gerprint data, is checked at ports of entry to confirm the identity of travelers. DHS has broad access to our entire CCD, which contains more than 143 million records, related to both immigrant and nonimmigrant visas, covering the last 13 years. 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 conduct visa security investigations overseas.

We make all of our visa information available to other U.S. Government agencies for law enforcement and counterterrorism purposes, and we specifically designed our systems to facilitate comprehensive data sharing with these entities. We give other agencies immediate access to more than 13 years of visa data for these purposes, and they use this access extensively. For example, in May 2011, over 23,000 officers from DHS, the Department of Defense (DoD), the FBI, DOJ, and the Department of Commerce submitted nearly 2 million queries on visa records in the course of conducting law enforcement and/or counterterrorism investigations.

Working in concert with DHS, we have proactively expanded biometric screening programs and integrated this expansion into existing overseas facilities. In partnership with DHS and the FBI, we have established the largest biometric screening program on the globe. We were a pioneer in the use of facial recognition techniques and remain a leader in operational use of this technology. Currently, more than 146 million images are enrolled in our facial recognition database. In 2009, we expanded use of facial recognition from a selected segment of visa applications to all visa applications, and we are now expanding our use of this technology to passport records. We are testing use of iris recognition technology in visa screening, making use of both identity and derogatory information collected by DOD. These efforts require intense on-going cooperation from other agencies. We have 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 a 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, and we have fraud screening operations using sophisticated database checks at both 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.

DS adds an important law enforcement element to the Department's visa procedures. There are currently 75 ARSO-I positions approved for 73 consular sections overseas specifically devoted to maintaining the integrity of the process. In 2010, DS approved 48 additional ARSO-I positions to work in consular sections overseas. They are complemented by officers working domestically on both visa and passport fraud criminal investigations and analysis. These highly-trained law enforcement professionals add another dimension to our border security efforts.

The multi-agency team effort, based upon broadly-shared information, provides a solid foundation for securing our borders. The interagency community continues to automate processes to reduce the possibility of human error while at the same time enhancing our border security screening capabilities.

We face an evolving threat of terrorism against the United States. The people and the tools we use to address this threat must be sophisticated and agile and must take into account the cultural and political environment in which threats arise. Our officers must be well-trained, motivated, and knowledgeable. Information obtained from these tools must be comprehensive and accurate. Our criteria for taking action must be clear and coordinated. The team we use for this mission must be the best. The Department has spent years developing the tools and personnel needed to properly execute the visa function overseas and remains fully committed to fulfilling its essential role on the border security team.

#### TRAINING FOREIGN PASSPORT OFFICIALS

As part of our fraud prevention efforts, CA is working with the International Narcotics and Law Enforcement Affairs (INL) Bureau through INL's International Law Enforcement Academy (ILEA) network to provide passport anti-fraud training to officials from foreign passport issuance agencies.

The first class was piloted September 7-9, 2011 in El Salvador, for officials from various Central American countries. The training is designed to improve the integrity of other countries' passport issuance by helping them institute organizations,

processes, and procedures for detecting fraudulent passport applications as part of their adjudication and issuance processes.

We plan to offer this training in 2012 at the ILEAs in Botswana and again in El Salvador.

#### FOREIGN PARTNER CAPACITY-BUILDING PROGRAMS

The Department regularly engages our foreign partners bilaterally, regionally, and on a multilateral basis to address the issue of terrorist transit. This engagement involves a range of activities, including the exchange of information in a variety of security channels, the execution of capacity-building programs on border and document security, the provision of border screening programs like the Terrorist Interdiction Program/Personal Identification Secure Comparison and Evaluation System (TIP/PISCES), and regular consultations on broader issues. Our capacity-building efforts are intended to foster regional cooperation and collaboration, whether through participation in organized regional groupings, such as the Trans-Sahara Counterterrorism Partnership, which facilitate regional training and exercises, or through assistance programs, such as the Regional Security Initiative (RSI), which funds regional Counterterrorism (CT) training and cooperative efforts across all CT priority regions.

The Department works in close coordination with the interagency community for the development and implementation of the full range of CT programming, through a range of fora. In addition to participation in regular National Security Council-led meetings, we have established mechanisms, such as the aforementioned RSI, which brings together our Embassy leadership with the full range of interagency representatives to discuss key issues of regional concern. This is replicated at the working level through the Regional Interagency Consultative Group. In North Africa, as already noted, we also have the Trans-Sahara Counterterrorism Partnership, through which State, DoD, and USAID cooperate and coordinate efforts to strengthen the counterterrorism capacity of our regional partners. The success of this approach has led to consideration of a similar construct for other regions. In addition to coordination through formal structures, we cooperate informally on a regular basis with the Departments of Defense, Justice, Homeland Security, and the Treasury on our counterterrorism efforts across the board.

#### U.S. GOVERNMENT EFFORTS TO STOP TERRORIST TRAVEL

The U.S. Government has many programs designed to thwart terrorist travel around the world. Many portions of the U.S. Government play a critical role in stopping terrorist travel—DHS and its components, DoD, the law enforcement and intelligence communities, and State Department consular officers.

U.S. passports and visas contain sophisticated security features that make them very difficult to forge. The electronic chips in our passports and the machine readable lines on our visas employ some of the most sophisticated technical security measures available. State Department consular officers work with our partners from CBP and ICE to train foreign border and airline personnel in the detection of fraudulent travel documents. The Department's Office of the Coordinator for Counterterrorism (S/CT) also helps foreign partners at risk for terrorist activity to establish their own computerized stop-list systems via the TIP/PISCES program.

In the additionally critical areas of international travel document security and interoperability, we have intensified our work. With passport-issuing authorities of International Civil Aviation Organization (ICAO) member States around the globe, we have striven to ensure that, as with the U.S. ePassport, other issuing authorities meet internationally established standards for security and interoperability. This has included the cooperative and growing use of the Public Key Directory (PKD), which is centrally managed and overseen by a board of actively participating ICAO member states. The PKD is a directory used by a receiving state to verify the digital signature used by a travel document's issuing authority, thereby authenticating the passport in real time.

The ePassports, which we have been issuing since December 2005, introduce a new class of security feature to identity documents: A digital signature. The validation of a signature guarantees that the chip contents, which include the facial image, are genuine and belong to the physical document. Only on this basis can it be proven that a specific ePassport was issued to the person that claims to be the rightful owner. The ICAO PKD is integral to the effort to have an efficient and commonly-accepted means of sharing and updating digital signatures (public keys) used by the world's ePassport-issuing authorities.

Where validation using the ICAO PKD occurs during travel, whether at points of embarkation, transit, or upon entry, it provides much greater levels of assurance

than are currently possible with traditional machine-readable travel documents. Border inspectors will be better able to identify inadequately documented travelers. Border inspectors worldwide can, in effect, assist the issuing authority in enhancing the integrity of all ePassports.

The benefits of the ICAO PKD increase exponentially as the number of States participating, and the number of ePassports in circulation, increase. Participating States and entities stand to benefit most, because their participation in the ICAO PKD maximizes global coverage of validation of their travel documents.

Electronically reading the PKI adds a third level of security for biometric passports, joining visual/tactile and laboratory features of the document, and scanner reading of the biometric content. This combination of features constitutes a tool bag for CBP officers to use in verifying the authenticity of the person and his/her passport when entering the United States.

The U.S. Government's advanced information-sharing initiatives ensure that we and our international partners are in constant contact regarding the threat of terrorist travel. CBP's use of Advance Passenger Information (API) and Passenger Name Record (PNR) data are valuable tools in detecting travel patterns and co-travelers of terrorist suspects. The U.S. Government's agreements with foreign partners under Homeland Security Presidential Directive (HSPD) 6 allow us to share terrorist screening information with trusted partners, in order to interdict known and suspected terrorists.

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 travelers based on biometric matching in some individual cases. 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. These arrangements would be limited to information regarding nationals of third countries. We expect both agreements to be completed this year, and similar agreements with Australia and New Zealand in 2012.

The Department plays a key role in all of these international initiatives. With our partners at the TSC, we negotiate the HSPD-6 agreements overseas. We are a close partner with DHS in API and PNR discussions overseas, in particular with respect to the current talks with the European Union on PNR. Together, all of these programs are helping achieve the goal of constraining terrorist mobility. This is our obligation to the American people.

#### CONCLUSION

We believe that U.S. interests in legitimate travel, trade promotion, and educational exchange are not in conflict with our border security agenda and, in fact, further that agenda in the long term. Our long-term interests are served by continuing the flow of commerce and ideas that are the foundations of prosperity and security. Acquainting people with American culture and perspectives remains the surest way to reduce misperceptions about the United States. Fostering academic and professional exchanges keeps our universities and research institutions at the forefront of scientific and technological change. We believe the United States must meet both goals to guarantee our long-term security.

Our 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. The Department of State is in a position to anticipate and weigh all those factors, while ensuring border security as our first priority.

The Department has developed and implemented an 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 frontline of border security. Each officer's experience 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.

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

Mrs. MILLER. Thank you very much. The Chairwoman now recognizes Mr. Cohen for his testimony.

**STATEMENT OF JOHN D. COHEN, DEPUTY COUNTERTERRORISM COORDINATOR, DEPARTMENT OF HOMELAND SECURITY**

Mr. COHEN. Thank you, Chairwoman Miller, Ranking Member Cuellar, Mr. Thompson, Members of the subcommittee. Thank you for the opportunity to be here today to discuss efforts to prevent terrorists from exploiting our visa system. As you have heard and as you pointed out yourself, through a combination of expanded and recurrent vetting of visa applicants, visa holders, as well as improved capabilities that I will describe in just a bit of vetting potential overstays, the ability of terrorists to exploit our visa systems has been greatly diminished.

Over the past 3 years Secretary Napolitano has made it a top priority for the Department through ICE, the efforts of ICE and CBP and US-VISIT, and our headquarters elements to improve our ability to vet prior to departure those traveling to the United States on visa or waiver country. We have made significant progress in leveraging the vast holdings of the intelligence community, the law enforcement community, and improve the information sharing and operational coordination between law enforcement, intelligence community, and those responsible for protecting our borders.

Today what I am about to describe is the next step in that process, because we have embarked on an effort to automate data queries that in the past were carried out through manual database checks. This is important because in many respects a big part of the problem and one of the main reasons that we had what were commonly referred to as backlog was because of the time-consuming nature that these database queries required. By interlinking immigration, National security, and law enforcement information systems, and better using intelligence-driven targeting capabilities such as those used at the National Targeting Center and through the automated targeting system, we have and will continue to bring greater efficiencies to this process, and this will allow for more effective use of personnel involved in investigations and analysis.

You referred to earlier, Madam Chairwoman, to the 1.2—750,000 records that had been unvetted. We began with 1.6 million records and through an initiative began earlier this year that involved CBP, ICE, US-VISIT, NCTC, and others we were able to eliminate from that 1.6 million records approximately 800,000 records that we were able to determine had actually departed the country or had changed their immigration status.

That left approximately 839,000 records that we were then able to vet through the holdings of the NTC and leveraging CBP's tech-

nical capabilities through a variety of law enforcement databases. Each one of those 839,000 records has been vetted from a National security and public safety perspective. Let me repeat that, the entire set of records in that 839,000 data set has been vetted from the National security and public safety perspective. Through this process, this automated and manual process, we have been able to provide to ICE, CTCEU, and ICE investigations several thousand additional leads which they have fully vetted, fully investigated and are in the process of completing their investigative processes. This was a significant milestone. We learned from that effort that we could do more to automate the process. Over the next 6 to 12 months you will see a number of improvements. We will further enhance our ability to prevent an onerous, suspected terrorist from exploiting the visa system or visa waiver program because we will be bringing automated processes to our ability to determine the location and the immigration status. We are seeking to eliminate to the greatest degree possible all of those manual database checks that are carried out in this country, that are carried out by visa security agents abroad. We will improve US-VISIT's ability to determine whether a person is in overstay status and quickly identify and forward to ICE investigators overstays are of a National security or public safety concern.

We will incorporate and enhance vetting capability that aggregates information for multiple systems into a unified electronic dossier, reducing the need for US-VISIT researchers and ICE agents to review multiple systems. We will be able to provide Congress country-by-country data on percentages of nationals who have overstayed their period of admission. We will establish a more complete, enhanced biographic exit system which includes expanded use of biometric data collected and retained in law enforcement immigration and DOD systems.

In addition to providing enhanced biographic exit capability, we will have established the foundation for a biometric exit capability. As resources become available and biometric collection technology continues to mature in the coming years, we will integrate those advances into this biographic exit foundation.

We are looking to leverage, as I pointed out, the same architecture into the visa protection program, allowing ICE to bring analytic responsibilities back home here to the United States, thereby allowing agents abroad to be more focused on investigative activities.

I appreciate again the opportunity to be here today, and I look forward to answering any questions. Thank you.

[The statement of Mr. Cohen follows:]

PREPARED STATEMENT OF JOHN D. COHEN

SEPTEMBER 13, 2011

INTRODUCTION

Chairwoman Miller, Ranking Member Cuellar, and distinguished Members, I am pleased to appear before you to outline the efforts of the Department of Homeland Security (DHS) to both prevent terrorists from entering the United States and ensure that our Visa System is secure.

I am testifying today in my role as the Principal Deputy Coordinator for Counterterrorism (CT) at the Department. In this capacity, I will address the Department's

efforts to enhance the security of the Visa System, and also discuss the creation and evolution of the CT Coordination functions at DHS. In addition, I will describe specific actions being taken by the National Protection and Programs Directorate's (NPPD's) United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program to complement the efforts of U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP), alongside whom I am pleased to be testifying today.

#### ENHANCING VISA SECURITY TO PREVENT TERRORIST TRAVEL

The Homeland Security Act of 2002 gave DHS the responsibility of preventing terrorists from entering the United States, providing the Department with the authority to establish and administer the rules that govern the granting of visas. This includes ensuring that the visa process is secure. Under this authority, DHS works closely with the Department of State to use the Visa System as a first layer of security to prevent known or suspected terrorists from traveling to the United States. Central to this mission is ensuring that consular officers at the State Department have necessary information, and then appropriately vet this information, which includes fingerprints and photographs, through the Department and our interagency partners.

Since 9/11, DHS has enhanced our Nation's ability to detect individuals seeking to exploit the visa system through recurrent vetting of visa holders. In May 2010, CBP's National Targeting Center—Passenger (NTC-P) implemented a new program to conduct continuous vetting of U.S. non-immigrant visas that have been recently issued, revoked, and/or denied. The Visa Hot List vetting ensures that changes in a traveler's visa status are identified in near real-time. If a violation is discovered, and the person is scheduled to travel to the United States, CBP will request that DOS revoke the visa and recommend to the airline that the person be denied boarding. If no imminent travel is identified, CBP will coordinate with DOS for a visa revocation, if appropriate. If the subject of an existing visa revocation initiated by the DOS or recommended by CBP is found to be in the United States, CBP will notify the Counterterrorism and Criminal Exploitation Enforcement Unit for further action.

In addition, since December 25, 2009, we have accelerated our efforts to synchronize, streamline, and advance the Department's overall vetting capability, which both increases security and efficiency. In particular, the Department is currently working to enhance screening efforts for those who have potentially overstayed their period of admission and modernize and enhance the Department's Biographic Exit architecture.

In May 2011, at the direction of Secretary Napolitano, DHS's CT Coordinator organized an effort to ensure that all overstays, regardless of priority, receive enhanced National security and public safety vetting by the National Counterterrorism Center (NCTC) and CBP.

NPPD/US-VISIT used automated means to review all records in the backlog by checking ADIS, CLAIMS, and I-94 holdings to reduce the backlog. As a result of this review, we identified 843,000 visa overstays who were no longer in the country. Then, both NCTC and CBP vetted the remaining 757,000 potential in-country overstay leads, along with 82,000 previously vetted overstay leads. CBP used its Automated Targeting System to query multiple databases, and to compare records to CBP's intelligence-based threshold targeting rules to identify indicators such as suspicious travel patterns or irregular travel behavior. Simultaneously, NCTC vetted the backlogged records through a number of databases held by the intelligence community.

By the end of July 2011, all of the previously un-reviewed possible overstays records had been reviewed from a National security and public safety standpoint and ICE is currently pursuing leads that meet our priorities.

This effort has increased the standard of review of overstay leads, at reduced cost. The process allows ICE to better prioritize targets for investigation and removal. It is a prime example of how increased coordination can help our Department to better leverage information and capabilities spread across the Department and the Federal Government.

The Department is nearing the final stages of developing a plan that not only institutionalizes these vetting enhancements, but also improves the current biographic exit system as well. We are focusing our efforts on improving information sharing, streamlining screening and vetting, and ensuring identification of potentially harmful individuals.

This plan includes many enhancements, including those which will allow DHS to:

- Quickly identify and forward to ICE investigators overstays that are of a National security concern.
  - Integrate and leverage relevant CBP, ICE, and US-VISIT information systems and operational processes to automate manual data queries and to vet DHS-held immigration and travel-related information against a broad array of law enforcement and IC data holdings.
  - Incorporate an enhanced vetting capability that aggregates information from multiple systems into a unified electronic dossier reducing the need for US-VISIT researchers and ICE agents to review multiple systems during their Validation and Vetting processes.
  - Take action against all overstays. DHS will forward information to the State Department for the purpose of cancelling visas of those who overstay. DHS will also eliminate the ability of those who overstay from using the Visa Waiver Program by cancelling any ESTA approvals or denying ESTA submissions for those who have overstayed. DHS will also place lookouts on individuals who overstay beyond certain statutory-identified time limits, so that they are inadmissible to the United States. DHS believes this will create a deterrent effect.
  - Provide to Congress country-by-country data on percentages of nationals who have overstayed their period of admission.
- DHS is committed to working with Congress to make these improvements. In addition to improving visa security, DHS has also implemented other measures to prevent another terrorist attack, including:
- Unifying immigration and border management systems to implement a more effective capability to access and employ biometric- and biographic-based information when reviewing possible terrorist travel.
  - Enhancing capabilities for identifying fraudulent documents and imposters and implementing measures to confirm the authenticity and validity of travel documents.
  - Establishing interoperability and information-sharing protocols with our Federal partners.
  - Supporting State and local law enforcement agencies and the intelligence community; using a more complete and accurate picture of a person's immigration, terrorist, and criminal history enables DHS to more effectively make connections in determining who might pose a threat or use more than one identity.
  - Establishing and maintaining strategic partnerships with an increasing number of international partners. In these partnerships, we share appropriate information, provide technical assistance, develop commonality in biometric standards and best practices, and investigate and test emerging biometric technologies.

#### THE ROLE OF THE COORDINATOR FOR COUNTERTERRORISM

Following the attempted bombing of Northwest flight 253 on December 25, 2009, Secretary Napolitano gave NPPD's Under Secretary Rand Beers the additional role of CT coordinator. The Department's CT Coordinator is responsible for coordinating all counterterrorism activities for the Department and across its directorates, components, and offices related to the detection, prevention, response to, and recovery from acts of terrorism.

In November 2010, DHS established the Counterterrorism Advisory Board (CTAB) to further improve coordination on counterterrorism among DHS Components. As the CT Coordinator, Under Secretary Beers serves as the chair of the CTAB, with the Under Secretary of Intelligence and Analysis (I&A) and the Assistant Secretary for Policy supporting the Board as Vice Chairs. Members include the leadership of TSA, CBP, ICE, the Federal Emergency Management Agency (FEMA), the U.S. Coast Guard (USCG), USCIS, the U.S. Secret Service (USSS), NPPD, and the Office of Operations Coordination and Planning (OPS). The DHS General Counsel serves as legal advisor to the CTAB.

In December 2010, the Department also established a counterterrorism working group, known as the CTWG, to support the CT Coordinator, and Secretary Napolitano later appointed me as Principal Deputy CT Coordinator.

The CTAB's mission is aligned with the Department's central mission: To prevent terrorist attacks and enhance security. The CT Coordinator, the CTAB, and the CTWG serve as the connective tissue that brings together the intelligence, operational, and policy-making elements within DHS Headquarters and the Components.

We rely on I&A to provide an understanding of potential threats and to coordinate with intelligence components within the Department and intelligence community. We then facilitate a cohesive and coordinated operational response, through the CTAB and other mechanisms, to deter and disrupt terrorist operations.

The CTAB is both headquarters- and Component-driven. Components have the opportunity to address the Secretary's priorities in an organized, coordinated fashion, but also use the CTAB to bring attention to their initiatives and priorities that need support from headquarters and other components. In addition, the CTAB fosters collaboration among Components and provides situational awareness of what each Component does and needs during a high-threat scenario. Similarly, we work with the DHS Office of Policy to address day-to-day and long-term strategy issues identified through this process and work to implement those changes.

Let me provide the following examples of how this process has worked over the last few months, with the offer to provide greater detail in a classified setting.

#### NPPD/US-VISIT

One of NPPD/US-VISIT's most important roles is to identify visitors to this country and to assist in the overall security of our immigration system.

NPPD/US-VISIT provides biometric identification and analysis services to distinguish people who pose a threat from the millions of people who travel for legitimate purposes. The program stores and analyzes biometric data—digital fingerprints and photographs—and links that data with biographic information to establish, and then verify, identities. NPPD/US-VISIT's IDENT, is the Department's biometric storage and matching service.

IDENT contains a watch list of more than 6.2 million known or suspected terrorists, criminals, and immigration violators. This capacity enables US-VISIT to provide homeland security decisionmakers with critical information when and where they need it. For example, this system can be utilized during by CBP primary screening during to run the fingerprints of foreign nationals against the watch list, with results returned in fewer than 10 seconds.

IDENT data, paired with biographic information from NPPD/US-VISIT's ADIS, supports decision-maker determinations as to whether foreign travelers should be prohibited from entering the United States; can receive, extend, change, or adjust immigration status; have overstayed or otherwise violated their authorized terms of admission; should be apprehended or detained for law enforcement action; or need special protection or attention, as in the case of refugees. Through ADIS, NPPD/US-VISIT can identify individuals who have overstayed their period of admission and then forward these leads to ICE for further action. In addition, IDENT plays a critical role in the biometric screening and identity verification of non-U.S. citizens for the State Department, ICE, CBP, USCIS, and the U.S. Coast Guard.

NPPD/US-VISIT's IDENT is fully interoperable with the Federal Bureau of Investigation's (FBI's) 10-fingerprint-based Integrated Automated Fingerprint Identification System (IAFIS). Daily transactions of FBI fingerprint data shared between IAFIS and IDENT number in the tens of thousands, providing the capability for FBI and NPPD/US-VISIT customers to simultaneously match biometrics against our system and watch list, as well as FBI data.

Enhanced interoperability with the FBI has enabled NPPD/US-VISIT to launch the Rapid Response capability, which allows CBP officers to search and receive a response against the FBI's entire criminal master file of more than 69 million identities, in near real-time, during primary inspection. Rapid Response is operational at four air ports of entry and is planned for Nation-wide deployment at air ports of entry next fiscal year.

DHS is also working closely with the Department of Defense (DOD) to increase information sharing and establish interoperability between IDENT and DOD's fingerprint database, the Automated Biometric Identification System. We currently have manual methods for sharing this data, which has helped DOD identify foreign combatants and match latent fingerprints retrieved from objects such as improvised explosive device fragments or collected from locations where terrorists have operated.

The goal is to have the U.S. Government's three largest biometric systems—those of NPPD/US-VISIT, the FBI, and DOD—completely interoperable, thereby enriching our data sets by making information sharing more seamless and automating the biometric-checking process to make it far more efficient. Even after complete interoperability has been achieved, the three systems will continue to be maintained and governed by each agency's respective policies, including those that ensure appropriate privacy safeguards are in place.

#### INTERNATIONAL COOPERATION AND COLLABORATION

DHS works extensively with foreign governments to increase information sharing to prevent terrorist travel at the earliest point possible. The Department is focused on sharing appropriate information, increasing system interoperability, providing



technical assistance, and establishing commonality in data and biometric standards and best practices. For instance, we are:

- Working with Mexican federal police and immigration authorities to identify and stop dangerous people from transiting to Mexico; enhancing efforts to combat transnational crime and confront organizations whose illicit actions undermine public safety, erode the rule of law, and threaten National security; and supporting Merida Initiative capacity-building programs such as the incorporation of biometrics into Mexico Immigration's Integrated System for Migration Operations. DHS has supported non-intrusive inspection equipment training, financial crimes investigative training, canine enforcement training, assistance in transitioning the Mexican Customs from a revenue-based institution to a law enforcement-based institution, and improvements in immigration control programs.
- Forging new partnerships with New Zealand, India, South Africa, the Republic of Korea, Germany, Spain, Greece, and the Dominican Republic to support their implementation of biometric systems.
- Sending technical experts to the United Kingdom, Australia, Canada, and, potentially, New Zealand, to help build biometric capabilities and develop more systematic methods for information sharing.
- Implementing the Preventing and Combating Serious Crime agreements to formalize sharing of biometric and limited biographic data under the U.S. Visa Waiver Program with Germany, Spain, the Republic of Korea, and other countries.
- Working with the International Civil Aviation Organization, the International Transport Association and INTERPOL to support the exchange of information and best practices and the establishment of standards in the areas of aviation security, identity management, emerging technologies, document security and verification, and fraud detection.

The Immigration Advisory Program (IAP) is another example of partnership between the Department, foreign governments, and commercial air carriers to identify and prevent high-risk, improperly-documented travelers from boarding U.S.-bound flights. IAP is currently in operation at eight airports in six countries. IAP officers have established strong working relationships with foreign law enforcement and counterterrorism officials and facilitated a direct link and real-time communication between foreign counterparts, the U.S. Embassy/Consulate, and the National Targeting Center.

DHS will continue to expand international coalitions to protect our Nation in the face of evolving terrorist threats, an increasingly interconnected global economy, and growing transnational crime. Along with our partners, we view cooperation, collaboration, and information sharing as critical in reaching our common goals of enhancing global security while facilitating legitimate travel and ensuring access to our economies.

#### SUCCESS STORIES

Information sharing among agencies and international partners continues to yield significant results, as demonstrated by these success stories:

- On February 3, 2011, the Australian Department of Immigration and Citizenship submitted a batch of fingerprints under the High Value Data Sharing Protocol of the Five Country Conference for matching against IDENT. The fingerprints of a subject applying for asylum in Australia matched an identity on the IDENT biometric watch list as a known or suspected terrorist in the FBI's Terrorist Screening Database. DHS contacted the FBI Counterterrorism Division and its Terrorist Explosives Device Analytical Center to confirm the subject's derogatory information. The FBI then notified Australian authorities. The individual was not granted asylum status in Australia based on this information.
- In November 2010, DHS assisted in a case involving an applicant for employment at a nuclear power plant. It was determined that the subject was using a false document under a false identity, in an attempt to demonstrate his legal status to reside and work in the United States. The subject was subsequently arrested by DHS law enforcement authorities as an overstay and placed into Federal custody awaiting removal proceedings.
- In October 2009, a vessel named Ocean Lady, transporting 76 undocumented persons, arrived off the coast of British Columbia, Canada. The intent of all individuals on board was to claim asylum status in Canada. The Canada Border Services Agency (CBSA) intercepted the vessel and worked with the ICE attaché in Ottawa to determine whether information on the identities of the individuals existed in U.S. systems. Pursuant to an existing agreement between

CBSA and DHS, the asylum claimants' fingerprints were submitted to NPPD/US-VISIT for a search. The fingerprint searches in IDENT identified two subjects as known or suspected terrorists and members of the Liberation Tigers of Tamil Eelam. Both subjects had also previously applied for U.S. nonimmigrant visas in 2008 and had been denied. Both subjects were denied asylum in Canada.

#### CONCLUSION

DHS is working hard to stop terrorists before they ever get to the United States. As we continue to work to address today's complex challenges, we will look for innovative ways to bridge gaps in information, technology, and human decision-making. Working with our partners; using common technologies, standards, and best practices; and sharing critical information will better protect us from those who seek to exploit our immigration systems. DHS is also cognizant that although physical security is of paramount concern and it is vital that we do everything possible to prevent terrorist travel, we must steadfastly seek to ensure that privacy, civil rights, and civil liberties are always protected. In developing and operating our programs, the Department's Office of Privacy and Office of Civil Rights and Civil Liberties are an integral part of the process.

By strengthening and increasing coordination within the Department, across the Federal Government, and with our international partners, we will develop and implement comprehensive measures that make efficient use of limited resources. With the appropriate coordination and structure within DHS Headquarters, we can better support our Operational Components as they work to enhance the security of our immigration systems while facilitating legitimate travel. In my role as Principal Deputy CT Coordinator for the Department, I look forward to continuing to work with you to address the challenges that remain.

Chairwoman Miller, Ranking Member Cuellar, and distinguished Members, thank you again for this opportunity to testify. I will be happy to answer any of your questions.

Mrs. MILLER. Thank you very much, Mr. Cohen. We look forward to questioning you on all of that new information you just gave us, so get ready.

Next the Chairwoman recognizes Mr. Edge.

#### **STATEMENT OF PETER T. EDGE, DEPUTY ASSOCIATE DIRECTOR, HOMELAND SECURITY INVESTIGATIONS, IMMIGRATION AND CUSTOMS ENFORCEMENT, DEPARTMENT OF HOMELAND SECURITY**

Mr. EDGE. Good morning, Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee. On behalf of Secretary Napolitano and Director Morton, thank you for the opportunity to discuss ICE's efforts to prevent the exploitation of our visa system by terrorists.

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

We are proud of the good work we have done over the last 10 years to protect the integrity of our visa system. ICE recognizes that those who pose National security threats often commit immigration benefit fraud while seeking to enter or remain in the United States, and we work hard to detect and deter immigration fraud by continually enhancing our anti-fraud efforts.

Working closely with Citizenship and Immigration Services, or CIS, ICE exercises criminal authority in the detection and deterrence of immigration fraud. While recognizing CIS's administrative authority, this strategy allows ICE to concentrate its effort on

major fraud conspiracies and other cases of National security or public safety interest while allowing CIS to address the bulk of immigration benefit fraud cases administratively.

As you know, the Homeland Security Act of 2002 directs DHS to assist in the identification of visa applicants who wish to enter the United States for illegitimate purposes, including illegal immigration, criminal activities, and terrorism-related activities. The visa adjudication process is often the first opportunity to assess whether a potential non-immigrant visitor or immigrant presents a threat to the United States.

The Visa Security Program is one of several ICE programs designed to minimize global risk. Our special agents in the Visa Security Program focus on select applicants who may have connections to terrorism or transnational criminal organizations. We then coordinate with the State Department to develop targeting plans based on the various threats. DHS does not participate in all of these adjudications, but rather becomes a part of the process following initial screening of an applicant where ICE's visa security operation happens to be present.

DHS actions compliment the consular office's initial screening, applicant interviews, and reviews of the applications and supporting documentation. ICE now conducts visa security operations at 19 high-risk visa adjudication posts in 15 countries. In fiscal year 2011 to date the Visa Security Program has screened over 900,000 visa applicants and, in collaboration with our State Department colleagues, determined that 130,000 require further review. Following the review of these 130,000 applicants, ICE identified derogatory information on more than 10,400 applicants. In every instance the State Department followed ICE's recommendation concerning the visa applicant.

A vulnerability that in the past had been exploited involved the acceptance of foreign students and visitors into the U.S. educational system. Helping to mitigate this vulnerability is ICE's Student and Exchange Visitor Program, or SEVP, which is a self-funded program based on fees collected from students, exchange visitors, and schools. This program certifies, recertifies, and decertifies schools' eligibility to sponsor foreign individuals for scholastic enrollment and other academic purposes. The SEVP acts as the bridge for Government organizations that have an interest in information on foreign students. SEVP helps DHS and the State Department to monitor schools and exchange programs regarding the visa classifications of F for academic and M for vocational and J for exchange category visitors.

SEVP administers the F and M student visa categories, while the State Department manages the J exchange visitor program. SEVP collects, maintains, and provides the information so that only legitimate foreign students or exchange visitors gain entry into and remain in the United States. SEVP uses the Student and Exchange Visitor Information System, or SEVIS, to track and monitor schools and programs, student exchange visitors and their dependents approved to participate in the U.S. education system.

SEVP interacts closely with ICE's Counterterrorism and Criminal Exploitation Unit, CTCEU, the first National program dedicated to the enforcement of nonimmigrant visa applications. Today

through the CTCEU, ICE proactively develops cases for investigation and cooperation with SEVP and the US-VISIT program.

As we move forward it is imperative that we expand the Nation's enforcement efforts concerning overstays and other status violations specifically regarding 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.

Ten years 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 I would appreciate your continued support of ICE and law enforcement. Thank you very much.

[The statement of Mr. Edge follows:]

PREPARED STATEMENT OF PETER T. EDGE

SEPTEMBER 13, 2011

INTRODUCTION

Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee: On behalf of Secretary Napolitano and Director Morton, thank you for the opportunity to discuss U.S. Immigration and Customs Enforcement's (ICE) efforts to prevent the exploitation of our visa system by terrorists. 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 entry into the United States and ensuring compliance with the conditions of such entry cannot be understated. We are proud of the good work we have done over the last 10 years to protect the integrity of our visa system, and I look forward to sharing with you both our successes thus far and the opportunities we see to improve our systems.

JOINT ANTI-FRAUD STRATEGY

We recognize that those who pose National security threats often commit immigration benefit fraud while seeking to enter or remain in the United States, and we work hard to detect and deter immigration fraud and to continually enhance our anti-fraud efforts. Working closely with U.S. Citizenship and Immigration Services (USCIS), ICE exercises criminal authority in the detection and deterrence of immigration fraud, while recognizing USCIS' administrative authority. This strategy allows ICE to concentrate its efforts on major fraud conspiracies and other cases of National security or public safety interest, while allowing USCIS to address the bulk of immigration benefit fraud cases administratively.

Through the ICE Document and Benefit Fraud Task Forces (DBFTFs), we focus our efforts on detecting, deterring, and disrupting document and benefit fraud. DBFTF participants include USCIS, the Department of State, the Department of Labor, and the Social Security Administration. Task Force investigators with expertise in different aspects of fraud collaborate with U.S. Attorneys' Offices around the country to formulate a comprehensive approach in targeting the criminal organizations and the beneficiaries behind these fraudulent schemes.

THE VISA SECURITY PROGRAM

The Homeland Security Act of 2002 directs DHS to assist in the identification of visa applicants who wish to enter the United States for illegitimate purposes, including illegal immigration, criminal activities, and terrorism-related activities. The visa adjudication process is often the first opportunity to assess whether a potential non-immigrant visitor or immigrant presents a threat to the United States. The Visa Security Program (VSP) is one of several ICE programs focused on minimizing global risks.

Our VSP Special Agents focus on select applicants and any connection the applicants may have to terrorism or transnational criminal organizations and coordinate with DOS to develop targeting plans based on assessed conditions and threats. The VSP ensures thorough reviews of applicants of concern in order to assess whether they pose a security threat to the United States. DHS does not participate in all

visa adjudications, but rather becomes a part of the process following initial screening of an applicant in countries where an ICE visa security operation is present. DHS actions complement the consular officers' initial screening, applicant interviews, and reviews of applications and supporting documentation.

ICE now conducts visa security operations at 19 high-risk visa adjudication posts in 15 countries. In fiscal year 2011 to date, the VSP has screened 900,000 visa applicants and, in collaboration with DOS colleagues, determined that 130,000 required further review. Following the review of these 130,000 applications, ICE identified derogatory information on more than 10,400 applicants. In every instance, DOS followed the VSP's recommendation concerning the visa applicant.

In March 2010 Customs and Border Protection's National Targeting Center (NTC) implemented a program to conduct continuous vetting of U.S. non-immigrant visas that have been recently issued, revoked, and/or denied. The continuous vetting ensures that changes in a traveler's visa status are identified in near real-time, allowing CBP to immediately determine whether to provide a no board recommendation to a carrier, recommend revocation of the visa to Department of State, or notify the ICE NTEU for individuals determined to be within the United States. Since the program's inception the Department of State has revoked more than 900 visas based on requests from CBP on information uncovered after a visa was issued.

Additionally, ICE has deployed VSP personnel to the NTC to augment and expand current operations. The NTC provides tactical targeting and analytical research in support of preventing terrorist and terrorist weapons from entering the United States. The co-location of VSP personnel at the NTC has helped increase both communication and information sharing. The NTC conducts pre-departure screening of all travelers on flights bound for the United States. Screening identifies high-risk passengers who should be denied boarding, including those whose visas have been revoked.

#### THE STUDENT AND EXCHANGE VISITOR PROGRAM (SEVP)

The Student and Exchange Visitor Program (SEVP) is a self-funded program based on fees collected from students, exchange visitors, and schools. It also certifies, recertifies, and decertifies schools' eligibility to sponsor foreign individuals for scholastic enrollment and other academic purposes. SEVP oversees reporting requirements and policies related to foreign nonimmigrant students and exchange visitors, and provide overall guidance to schools regarding SEVIS.

SEVP acts as the bridge for Government organizations that have an interest in information on foreign students. SEVP helps DHS and DOS monitor schools and exchange programs, as well as F (academic), M (vocational), and J (exchange) category visitors. SEVP administers the F and M student visa categories, while DOS manages the J exchange visitor program.

SEVP collects, maintains, and provides the information so that only legitimate foreign students or exchange visitors gain entry to, and remain in, the United States. The result is an easily accessible information system that provides timely information to DOS, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services and ICE. SEVP has a mutual commitment of shared responsibility with the educational community to maintain support and cooperation. Currently, SEVP has certified over 10,360 schools.

SEVP uses the Student and Exchange Visitor Information System (SEVIS) to track and monitor schools and programs, students, exchange visitors, and their dependents approved to participate in the U.S. education system.

#### THE COUNTERTERRORISM AND CRIMINAL EXPLOITATION UNIT (CTCEU)

The Counterterrorism and Criminal Exploitation Unit is the first 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 of hundreds of thousands of potential status violators, after analysis of data from SEVIS and US-VISIT, along with other information. These records are resolved by further establishing potential violations that would warrant field investigations, establishing compliance, or establishing departure dates from the United States. Between 15,000 and 20,000 of these records are resolved by in-house analysts each month. Since the creation of the CTCEU in 2003, analysts have resolved more than 1.6 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, resulting in over 1,400 administrative arrests per year.

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 initiating or supporting high-priority National security initiatives based upon specific intelligence. The practice is designed to detect and 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 identification approach based upon country of birth, gender, and age.

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 tri-annual 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.

A recent ICE investigation in Las Cruces, New Mexico, highlights how the CTCEU functions. As a result of CTCEU data analysis and field investigation, in February 2010, ICE Special Agents arrested two foreign nationals who were admitted as F-1 nonimmigrant students and violated the terms and conditions of their admission. Both individuals were referred for investigation after their status was terminated in SEVIS for failure to maintain student status, as well as for possessing several indicators of National security concerns.

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 student status to nonimmigrants, without requiring them to maintain full courses of study in order to comply with the terms of their admission. ICE's primary goal in these types of investigations is to focus on the criminal violations of the owner/operators of these businesses and the administrative violations on the students. This ICE investigation uncovered information that only approximately 5 percent of the school's students attended class on any given day. In addition to the indictment, follow-up investigation by ICE resulted in the administrative arrests of 116 student visa violators purported to be attending the school from countries including Thailand, Syria, Honduras, South Korea, Japan, Colombia, the Dominican Republic, Turkmenistan, Turkey, Indonesia, Venezuela, Brazil, and Kyrgyzstan.

As we move forward, it is imperative that we expand the Nation's enforcement efforts concerning overstays and other status violations specifically regarding 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.

#### 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 (NPPD). US-VISIT supports DHS's mission to protect our Nation by providing biometric identification services to Federal, State, and local government decisionmakers 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. Biometric information sharing between the Federal Bureau of Investigation's Criminal Justice Information Services and US-VISIT is the foundation of ICE's Secure Communities IDENT/IAFIS Interoperability Program.

Through Secure Communities, aliens—including those who have overstayed or otherwise violated their immigration status—who are encountered by law enforcement may be identified as immigration violators when criminally arrested by State and local law enforcement. Once individuals are identified through Secure Communities, ICE officials determine what enforcement action is appropriate, consistent

with ICE's enforcement priorities. Currently, Secure Communities is deployed in over 1,500 jurisdictions in 44 States.

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 Data Integrity Group (DIG) from three unique sources, which includes the typical overstay violation; a biometric watch list notification and a CTCEU Visa Waiver Enforcement Program (VWEP) nomination. 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.

A second type of lead is generated from biometric data collected by US-VISIT. US-VISIT routinely receives fingerprint records from a variety of Governmental sources and adds them to a biometric watch list that includes individuals of National security concern. These new watch list records are checked against all fingerprints in the US-VISIT's biometric database, the Automated Biometric Identification System, or IDENT, managed by US-VISIT, 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 non-immigrant 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 overstays arising from this VWP population given the large number of individuals in this category. Prior to the implementation of the VWEP in 2008, there was no National program dedicated to addressing overstays within this population. CTCEU provides a refined weekly list of individuals to US-VISIT for additional scrutiny, who have been identified as potential overstays who entered the United States under the VWP. In accord with its intelligence-based criteria, a relevant portion of this report is then imported into the CTCEU's internal lead tracking system for review and possible field assignment.

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

#### ICE'S PRESENCE OVERSEAS

Stopping a threat before it reaches our shores is an important priority that ICE supports internationally. Through our Office of International Affairs (OIA), we have personnel in 70 offices in 47 countries. ICE personnel in these offices collaborate with our foreign counterparts and Federal partner agencies in joint efforts to disrupt and dismantle transnational criminal organizations engaged in money laundering, contraband smuggling, weapons proliferation, forced child labor, human rights violations, intellectual property rights violations, child exploitation, human smuggling and trafficking, and many other violations. Additionally, ICE facilitates the repatriation of individuals with final orders of removal, returning violators to their home countries.

#### OVERSEAS 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; coordi-

nating meetings, training, and briefings; and engaging in regular and timely information sharing. The VSP's presence at 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 assist Consular Officers and other U.S. Government personnel to recognize 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

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 a few 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 other 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.

More recently, in May 2011, ICE Special Agents within the VSP Security Advisory Opinion Unit (SAOU) investigated a Saudi Arabian national who obtained a non-immigrant 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

Ten years 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 you, Mr. Edge. You certainly do have our continued support, and now the Chairwoman recognizes Mr. Stana.

#### **STATEMENT OF RICHARD M. STANA, DIRECTOR, HOMELAND SECURITY AND JUSTICE, GOVERNMENT ACCOUNTABILITY OFFICE**

Mr. STANA. Thank you, Chairwoman Miller and Mr. Cuellar, for the invitation to testify at today's hearing about GAO's work on this very important topic, the integrity and security of our visa processes.

As you know, each year millions of visitors come to the United States legally for a temporary visit. In the 6-year period from fiscal year 2005 to 2010 there were 36 million nonimmigrant visas issued for things like pleasure, business travel, student exchanges and so on, among other things. In addition, during that same period over



98 million visitors were admitted to the United States under the visa waiver program.

While most visa abusers you might say are motivated by economic opportunities to enter the United States and work, there are other National security consequences. As was mentioned earlier, 5 of the 19, 9/11 hijackers were here on one or the other overstay category, and 36 of 400 individuals convicted in international terrorism-related investigations by the Department of Justice were overstays.

As you have heard from the other panelists, both DHS and State have made some progress in shoring up our visa processes. I would like to discuss three areas from my prepared statement which could possibly add some context to what you have heard.

First, let's talk about the problem. We have overstays whether the person was admitted to the U.S. on a valid visa or through the visa waiver program. As was previously mentioned, the Pew Hispanic Center has estimated that about 40 percent of the total illegal alien population in the United States came in legally through a visa. On average that is about 4 in 10 and contrast the resources that we spend on interior enforcement with what we spend on the 60 percent for border enforcement, a big difference.

To its credit, as you heard, ICE uses a risk management approach to focus its limited resources on overstays leads that it considers most likely to pose a threat to National security or public safety. But that said, ICE averages only about 1,200 overstay arrests per year and devotes a little more than 3 percent of its investigative resources to overstays.

Now to be fair, finding overstays can be difficult, they don't self-advertise. Sometimes they leave the United States, sometimes they are now on status, sometimes they simply cannot be located. There are other programs that ICE and other DHS components operate, like work site enforcement and secure communities that do address overstays or overstays are a component of those programs. But when you add it all up, you take all those programs together, we are not making much of a dent in that 40 percent of the illegal alien population.

Moving forward, ICE expressed interest in increasing the resources to overstay investigations and assigning some responsibilities to ERO. But they haven't established time frames yet or identified the resources to make this happen.

My second point involves the US-VISIT system. There's good news and not so good news. The good news is it is operating 300 air, sea, and land ports of entry and it seems to be working well. It gathers biometric information which can enable DHS to identify travelers, check law enforcement databases, and prescreens others.

The not-so-good news is that it has only a very limited capability to process exit records currently. The exit process now includes processing air carriers, electronic submissions of manifest data and other biographic information as well as inconsistent collection of I-94s. So all told, it is not in a position right now to reliably state who has overstayed their visa and remains in the country.

As of July, this past July, US-VISIT obligated about \$193 million to develop air, sea, and land exit solutions since 2002. They had different types of exit solutions and piloted them, but all have

been determined to be insufficient and incomplete. There are some other arrangements being discussed now, such as with the Canadians, to make their exit as a person leaving the United States going into a Canada become our—their entrance become our exit and share information. But those agreements have not been formalized and there is more work that remains.

Finally, let's turn to the issue of ensuring visa integrity and security overseas. ICE has deployed agents to certain embassies and consulates as part of its Visa Security Program, as you have heard, but at some posts we found that guidance, training, and standard operating procedures were not established, which led to tensions between ICE and State, as well as operational inconsistencies. We also found that while ICE had a presence at 19 posts in 15 countries; it did not have agents located at 11 of the top 20 high-risk posts. You know, expanding the program can be limited by embassy space and budget consideration, but ICE has not acted on possible alternatives. Although I am listening to some of my fellow panelists this morning, it sounds like perhaps that information is superseded and there are steps to be taken to expand their vetting and screening processes.

On the positive side we heard about ESTA a few minutes ago. ESTA was implemented without many glitches. They are screening about 99 percent of the travelers coming into the United States on visa. However, there were about, I believe it was about 350,000 travelers who were boarded on airplanes without having a verified ESTA document and of those about 650 of those it was later found should not have been permitted to board the airplane. DHS has yet to analyze these cases to see if these were of legitimate concern or there were systematic weaknesses that need to be addressed for the program.

That concludes my statement. It is important to balance visa security responsibilities with a need to enhance travel, and we have made a number of recommendations to both State and DHS to help this happen.

Thank you very much.

[The statement of Mr. Stana follows:]

PREPARED STATEMENT OF RICHARD M. STANA

SEPTEMBER 13, 2011

GAO HIGHLIGHTS

Highlights of GAO-11-910T, a testimony before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives.

*Why GAO Did This Study*

The attempted bombing of an airline on December 25, 2009, by a Nigerian citizen with a valid U.S. visa renewed concerns about the security of the visa process. Further, unauthorized immigrants who entered the country legally on a temporary basis but then overstayed their authorized periods of admission—overstays—could pose homeland security risks. The Department of Homeland Security (DHS) has certain responsibilities for security in the visa process and for addressing overstays. DHS staff review visa applications at certain Department of State overseas posts under the Visa Security Program. DHS also manages the Visa Waiver Program through which eligible nationals from certain countries can travel to the United States without a visa. This testimony is based on GAO products issued in November 2009, August 2010, and from March to May 2011. As requested, this testimony addresses the following issues: (1) Overstay enforcement efforts, (2) efforts to imple-

ment a biometric exit system and challenges with the reliability of overstay data, and (3) challenges in the Visa Security and Visa Waiver programs.

*What GAO Recommends*

GAO has made recommendations in prior reports that, among other things, call for DHS to strengthen management of overstay enforcement efforts, mechanisms for collecting data from foreign nationals departing the United States, and planning for addressing certain Visa Security and Visa Waiver programs' risks. DHS generally concurred with these recommendations and has actions planned or underway to address them.

VISA SECURITY: ADDITIONAL ACTIONS NEEDED TO STRENGTHEN OVERSTAY ENFORCEMENT AND ADDRESS RISKS IN THE VISA PROCESS

*What GAO Found*

Federal agencies take actions against a small portion of the estimated overstay population, but strengthening planning and assessment of overstay efforts could improve enforcement. Within DHS, U.S. Immigration and Customs Enforcement's (ICE) Counterterrorism and Criminal Exploitation Unit (CTCEU) is the lead agency responsible for overstay enforcement. CTCEU arrests a small portion of the estimated overstay population in the United States because of, among other things, ICE's competing priorities, but ICE expressed an intention to augment its overstay enforcement resources. From fiscal years 2006 through 2010, ICE reported devoting about 3 percent of its total field office investigative hours to CTCEU overstay investigations. ICE was considering assigning some responsibility for noncriminal overstay enforcement to its Enforcement and Removal Operations directorate, which apprehends and removes aliens subject to removal from the United States. In April 2011, GAO reported that by developing a time frame for assessing needed resources and using the assessment findings, as appropriate, ICE could strengthen its planning efforts. Moreover, in April 2011, GAO reported that CTCEU tracked various performance measures, but did not have a mechanism to assess the outcomes of its efforts. GAO reported that by establishing such a mechanism, CTCEU could better ensure that managers have information to assist in making decisions.

DHS has not yet implemented a comprehensive biometric system to match available information (e.g., fingerprints) provided by foreign nationals upon their arrival and departure from the United States and faces reliability issues with data used to identify overstays. GAO reported that while the United States Visitor and Immigrant Status Indicator Technology Program's biometric entry capabilities were operating at ports of entry, exit capabilities were not, and DHS did not have a comprehensive plan for biometric exit implementation. DHS conducted pilots to test two scenarios for an air exit solution in 2009, and in August 2010, GAO concluded that the pilots' limitations, such as limitations not defined in the pilot evaluation plan like suspending exit screening at departure gates to avoid flight delays, curtailed DHS's ability to inform a decision for a long-term exit solution. Further, in April 2011, GAO reported that there is not a standard mechanism for nonimmigrants departing the United States through land ports of entry to remit their arrival and departure forms. Such a mechanism could help DHS obtain more complete departure data for identifying overstays.

GAO identified various challenges in the Visa Security and Visa Waiver programs related to planning and assessment efforts. For example, in March 2011, GAO found that ICE developed a plan to expand the Visa Security Program to additional high-risk posts, but ICE had not fully adhered to the plan or kept it up to date. Further, ICE had not identified possible alternatives that would provide the additional security of Visa Security Program review at those high-risk posts that do not have a program presence. In addition, DHS implemented the Electronic System for Travel Authorization (ESTA) to meet a statutory requirement intended to enhance Visa Waiver Program security and took steps to minimize the burden on travelers to the United States added by the new requirement. However, DHS had not fully evaluated security risks related to the small percentage of Visa Waiver Program travelers without verified ESTA approval.

Chairwoman Miller, Ranking Member Cuellar, and Members of the subcommittee: I am pleased to be here today to discuss the Department of Homeland Security's (DHS) programs and efforts to strengthen the security of the visa process, including efforts to identify and take enforcement against overstays—individuals who were admitted to the United States legally on a temporary basis—either with a visa, or in some cases, as visitors who were allowed to enter without a visa—but then over-

stayed their authorized periods of admission.<sup>1</sup> The attempted bombing of Northwest Airlines flight 253 on December 25, 2009, by a Nigerian citizen in possession of a valid U.S. visa renewed concerns about the security of the visa process. Each year, millions of visitors come to the United States legally on a temporary basis. From fiscal year 2005 through fiscal year 2010, the Department of State issued over 36 million nonimmigrant visas for business travel, pleasure, tourism, medical treatment, or for foreign and cultural exchange student programs, among other things.<sup>2</sup> In addition, from fiscal year 2005 through fiscal year 2010, over 98 million visitors were admitted to the United States under the Visa Waiver Program, which allows nationals from certain countries to apply for admission to the country as temporary visitors for business or pleasure without first obtaining a visa from a U.S. consulate abroad.<sup>3</sup>

Further, the most recent estimates from the Pew Hispanic Center approximated that in 2006, out of an unauthorized resident alien population of 11.5 million to 12 million in the United States, about 4 million to 5.5 million were overstays.<sup>4</sup> In February 2008, we reported that most overstays are likely motivated by economic opportunities to stay in the United States beyond their authorized periods of admission.<sup>5</sup> Individuals overstaying their authorized periods of admission could pose homeland security concerns. For example, in some instances overstays have been identified as terrorists or involved in terrorist-related activity, such as 5 of the 19 September 11, 2001, hijackers. Further, according to DHS data, of approximately 400 individuals reported by the Department of Justice as convicted in the United States as a result of international terrorism-related investigations conducted from September 2001 through March 2010, approximately 36 were overstays.<sup>6</sup>

DHS has certain responsibilities for strengthening security in the visa process, including identifying and taking enforcement action to address overstays. Within DHS, U.S. Customs and Border Protection (CBP) is tasked with, among other duties, inspecting all people applying for entry to the United States to determine their admissibility to the country and screening Visa Waiver Program applicants to determine their eligibility to travel to the United States under the program. U.S. Immigration and Customs Enforcement (ICE) is the lead agency for enforcing immigration law in the interior of the United States and is primarily responsible for overstay enforcement, and within ICE, the Counterterrorism and Criminal Exploitation Unit (CTCEU) is primarily responsible for overstay investigations. The United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT) within DHS's National Protection and Programs Directorate supports the identifica-

<sup>1</sup>Visitors who are allowed to seek admission without a visa include citizens of Canada and the British Overseas Territory of Bermuda (and certain residents of other adjacent islands, such as the Bahamas) under certain circumstances, as well as Visa Waiver Program participants (see footnote 3). In-country overstays refer to nonimmigrants who have exceeded their authorized periods of admission and remain in the United States without lawful status, while out-of-country overstays refer to individuals who have departed the United States but who, on the basis of arrival and departure information, stayed beyond their authorized periods of admission.

<sup>2</sup>Temporary visitors to the United States generally are referred to as "nonimmigrants." For a listing and descriptions of nonimmigrant categories, see 8 U.S.C. § 1101(a)(15); see also 8 C.F.R. § 214.1(a)(1)–(2). Generally, nonimmigrants wishing to visit the United States gain permission to apply for admission to the country through one of two ways. First, those eligible for the Visa Waiver Program apply on-line to establish eligibility to travel under the program prior to departing for the United States (unless they are seeking admission at a land port of entry, in which case eligibility is established at the time of application for admission). Second, those not eligible for the Visa Waiver Program and not otherwise exempt from the visa requirement must visit the U.S. consular office with jurisdiction over their place of residence or, in certain circumstances, the area in which they are physically present but not resident, to obtain a visa. Upon arriving at a port of entry, nonimmigrants must undergo inspection by U.S. Customs and Border Protection officers, who determine whether or not they may be admitted into the United States.

<sup>3</sup>In order to qualify for the Visa Waiver Program, a country must meet various requirements, such as entering into an agreement with the United States to report lost or stolen passports within a strict time limit and in a manner specified in the agreement. Currently, 36 countries participate in the Visa Waiver Program: Andorra, Australia, Austria, Belgium, Brunei, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, and the United Kingdom.

<sup>4</sup>Pew Hispanic Center, *Modes of Entry for the Unauthorized Migrant Population* (Washington, DC: May 22, 2006).

<sup>5</sup>GAO, *Visa Waiver Program: Limitations with Department of Homeland Security's Plan to Verify Departure of Foreign Nationals*, GAO-08-458T (Washington, DC: Feb. 28, 2008).

<sup>6</sup>For more information on these convictions, see Department of Justice, *National Security Division Statistics on Unsealed International Terrorism and Terrorism-Related Convictions* (Washington, DC: March 2010).

tion of nonimmigrant overstays. In 2002, DHS initiated the US-VISIT Program to develop a comprehensive entry and exit system to collect biometric data from aliens traveling through U.S. ports of entry. In 2004, US-VISIT initiated the first step of this program by collecting biometric data on aliens entering the United States. Further, the Department of State is responsible for issuing visas to foreign nationals seeking admission to the United States. In addition, DHS has responsibility for managing the Visa Security Program and the Visa Waiver Program. Specifically, ICE oversees the Visa Security Program under which it deploys officials to certain U.S. embassies and consulates to strengthen the visa process by working with Department of State officials in reviewing visa applications.<sup>7</sup> DHS is also responsible for establishing visa policy, including policy for the Visa Waiver Program.

As requested, my testimony will cover the following key issues: (1) Efforts to take enforcement action against overstays and reported results; (2) DHS's efforts to implement a biometric exit system and the reliability of data used to identify overstays; and (3) challenges and weaknesses in the Visa Security and Visa Waiver programs. This testimony is based on our prior work on overstay enforcement efforts, the US-VISIT program, the Visa Security Program, and the Visa Waiver Program. We issued reports from these efforts in April 2011, August 2010 and November 2009, March 2011, and May 2011, respectively.<sup>8</sup> For these reports, we examined program documentation, such as standard operating procedures, guidance for investigations, and implementation plans. We also interviewed DHS and Department of State officials. Additional details on the scope and methodology are available in our published reports. We conducted this work in accordance with generally accepted government auditing standards.

In summary, DHS has taken action to strengthen security in the visa process, but operational and management weaknesses have hindered the effectiveness of these efforts. First, ICE investigates and arrests a small portion of the estimated overstay population in the United States because of, for example, competing enforcement priorities. ICE also reported allocating a small percentage of its investigative work hours to overstay investigations since fiscal year 2006, but the agency has expressed an intention to augment the resources it dedicates to overstay enforcement efforts moving forward. However, ICE does not yet have a target time frame for completing its planning efforts for augmenting overstay enforcement resources, and it lacks mechanisms for assessing the effectiveness of its enforcement efforts. Second, DHS has not yet implemented a comprehensive biometric entry and exit system for collecting biometric data on foreign nationals when they depart the United States. In the absence of such a system, DHS uses primarily biographic data to identify overstays. However, unreliable data hinder DHS's efforts to accurately identify overstays. Third, ICE has deployed agents to certain embassies and consulates as part of the Visa Security Program, but has not performed mandated training, has faced staffing challenges, and has not fully adhered to its program expansion plan. DHS has taken action to strengthen the security of the Visa Waiver Program, but has not fully analyzed program risks or completed required reports on participating countries' security risks in a timely manner. We made a number of recommendations to DHS to strengthen its efforts in these areas, such as improving its management and assessment of overstay enforcement efforts, planning for a biometric exit capability and mechanisms for collecting data from foreign nationals departing the United States at land ports of entry, and addressing risks in the Visa Security and Visa Waiver programs. DHS concurred with these recommendations and has actions planned or under way to address them.

<sup>7</sup> The Homeland Security Act of 2002 (Pub. L. 107-296, 116 Stat. 2135) established DHS and gave the Secretary of Homeland Security authority to issue regulations with respect to the issuance and refusal of visas. Section 428 of the Homeland Security Act authorizes the Secretary of Homeland Security to assign DHS employees to consular posts overseas to support the visa process through various functions. See 6 U.S.C. § 236(e).

<sup>8</sup> GAO, *Overstay Enforcement: Additional Mechanisms for Collecting, Assessing, and Sharing Data Could Strengthen DHS's Efforts but Would Have Costs*, GAO-11-411 (Washington, DC: April 15, 2011); *Homeland Security: US-VISIT Pilot Evaluations Offer Limited Understanding of Air Exit Options*, GAO-10-860 (Washington, DC: Aug. 10, 2010); *Homeland Security: Key US-VISIT Components at Varying Stages of Completion, but Integrated and Reliable Schedule Needed*, GAO-10-13 (Washington, DC: Nov. 19, 2009); *Border Security: DHS's Visa Security Program Needs to Improve Performance Evaluation and Better Address Visa Risk Worldwide*, GAO-11-315 (Washington, DC: Mar. 31, 2011), and *Visa Waiver Program: DHS Has Implemented the Electronic System for Travel Authorization, but Further Steps Needed to Address Potential Program Risks*, GAO-11-335 (Washington, DC: May 5, 2011).

FEDERAL AGENCIES TAKE ACTIONS AGAINST A SMALL PORTION OF THE ESTIMATED  
OVERSTAY POPULATION

*ICE Investigates Few In-Country Overstays, but Its Efforts Could Benefit from Improved Planning and Performance Management*

As we reported in April 2011, ICE CTCEU investigates and arrests a small portion of the estimated in-country overstay population due to, among other things, ICE's competing priorities; however, these efforts could be enhanced by improved planning and performance management. CTCEU, the primary Federal entity responsible for taking enforcement action to address in-country overstays, identifies leads for overstay cases; takes steps to verify the accuracy of the leads it identifies by, for example, checking leads against multiple databases; and prioritizes leads to focus on those the unit identifies as being most likely to pose a threat to National security or public safety. CTCEU then requires field offices to initiate investigations on all priority, high-risk leads it identifies.

According to CTCEU data, as of October 2010, ICE field offices had closed about 34,700 overstay investigations that CTCEU headquarters assigned to them from fiscal year 2004 through 2010.<sup>9</sup> These cases resulted in approximately 8,100 arrests (about 23 percent of the 34,700 investigations), relative to a total estimated overstay population of 4 million to 5.5 million.<sup>10</sup> About 26,700 of those investigations (or 77 percent) resulted in one of these three outcomes:<sup>11</sup> (1) Evidence is uncovered indicating that the suspected overstay has departed the United States; (2) evidence is uncovered indicating that the subject of the investigation is in-status (e.g., the subject filed a timely application with the United States Citizenship and Immigration Services (USCIS) to change his or her status and/or extend his or her authorized period of admission in the United States); or (3) CTCEU investigators exhaust all investigative leads and cannot locate the suspected overstay.<sup>12</sup> Of the approximately 34,700 overstay investigations assigned by CTCEU headquarters that ICE field offices closed from fiscal year 2004 through 2010, ICE officials attributed the significant portion of overstay cases that resulted in a departure finding, in-status finding, or with all leads being exhausted generally to difficulties associated with locating suspected overstays and the timeliness and completeness of data in DHS's systems used to identify overstays.

Further, ICE reported allocating a small percentage of its resources in terms of investigative work hours to overstay investigations since fiscal year 2006, but the agency expressed an intention to augment the resources it dedicates to overstay enforcement efforts moving forward. Specifically, from fiscal years 2006 through 2010, ICE reported devoting from 3.1 to 3.4 percent of its total field office investigative hours to CTCEU overstay investigations. ICE attributed the small percentage of investigative resources it reported allocating to overstay enforcement efforts primarily to competing enforcement priorities. According to the ICE Assistant Secretary, ICE has resources to remove 400,000 aliens per year, or less than 4 percent of the estimated removable alien population in the United States. In June 2010, the Assistant Secretary stated that ICE must prioritize the use of its resources to ensure that its efforts to remove aliens reflect the agency's highest priorities, namely non-immigrants, including suspected overstays, who are identified as high-risk in terms of being most likely to pose a risk to National security or public safety. As a result, ICE dedicated its limited resources to addressing overstays it identified as most

<sup>9</sup>CTCEU also investigates suspected Visa Waiver Program overstays, out-of-status students and violators of the National Security Entry-Exit Registration System, a program that requires certain visitors or nonimmigrants to register with DHS for National security reasons. For the purpose of this discussion, these investigations are referred to collectively as "overstay" investigations. In addition to CTCEU investigative efforts, other ICE programs within Enforcement and Removal Operations may take enforcement action against overstays, though none of these programs solely or directly focus on overstay enforcement. For example, if the Enforcement and Removal Operations Criminal Alien Program identifies a criminal alien who poses a threat to public safety and is also an overstay, the program may detain and remove that criminal alien from the United States.

<sup>10</sup>The most recent estimates from the Pew Hispanic Center approximated that, in 2006, out of an unauthorized resident alien population of 11.5 million to 12 million in the United States, about 4 million to 5.5 million were overstays. Pew Hispanic Center, *Modes of Entry for the Unauthorized Migrant Population* (Washington, DC: May 22, 2006).

<sup>11</sup>Investigations resulting and not resulting in arrest do not total 34,700 due to rounding.

<sup>12</sup>With regard to the second outcome, that the subject is found to be in-status, under certain circumstances, an application for extension or change of status can temporarily prevent a visitor's presence in the United States from being categorized as unauthorized. See Donald Neufeld, Acting Associate Director, Domestic Operations Directorate, USCIS, "Consolidation of Guidance Concerning Unlawful Presence for Purposes of Sections 212(a)(9)(B)(i) and 212(a)(9)(C)(i)(I) of the [Immigration and Nationality] Act," memorandum, Washington, DC, May 6, 2009.

likely to pose a potential threat to National security or public safety and did not generally allocate resources to address suspected overstays that it assessed as non-criminal and low-risk. ICE indicated that it may allocate more resources to overstay enforcement efforts moving forward and that it planned to focus primarily on suspected overstays whom ICE has identified as high-risk or who recently overstayed their authorized periods of admission.

ICE was considering assigning some responsibility for noncriminal overstay enforcement to its Enforcement and Removal Operations (ERO) directorate, which has responsibility for apprehending and removing aliens who do not have lawful immigration status from the United States. However, ERO did not plan to assume this responsibility until ICE assessed the funding and resources doing so would require. ICE had not established a time frame for completing this assessment. We reported in April 2011 that by developing such a time frame and utilizing the assessment findings, as appropriate, ICE could strengthen its planning efforts and be better positioned to hold staff accountable for completing the assessment. We recommended that ICE establish a target time frame for assessing the funding and resources ERO would require in order to assume responsibility for civil overstay enforcement and use the results of that assessment. DHS officials agreed with our recommendation and stated that ICE planned to identify resources needed to transition this responsibility to ERO as part of its fiscal year 2013 resource-planning process.

Moreover, although CTCEU established an output program goal and target, and tracked various performance measures, it did not have a mechanism in place to assess the outcomes of its efforts, particularly the extent to which the program was meeting its mission as it relates to overstays—to prevent terrorists and other criminals from exploiting the Nation's immigration system. CTCEU's program goal is to prevent criminals and terrorists from exploiting the immigration system by proactively developing cases for investigation, and its performance target is to send 100 percent of verified priority leads to field offices as cases.<sup>13</sup> CTCEU also tracks a variety of output measures, such as the number of cases completed their associated results (i.e., arrested, departed, in-status, or all leads exhausted) and average hours spent to complete an investigation. While CTCEU's performance target permits it to assess an output internal to the program—the percentage of verified priority leads it sends to field offices for investigation—it does not provide program officials with a means to assess the impact of the program in terms of preventing terrorists and other criminals from exploiting the immigration system. We reported that by establishing such mechanisms, CTCEU could better ensure that managers have information to assist in making decisions for strengthening overstay enforcement efforts and assessing performance against CTCEU's goals. In our April 2011 report, we recommended that ICE develop outcome-based performance measures—or proxy measures if program outcomes cannot be captured—and associated targets on CTCEU's progress in preventing terrorists and other criminals from exploiting the Nation's immigration system. DHS officials agreed with our recommendation and stated that ICE planned to work with DHS's National security partners to determine if measures could be implemented.

*The Department of State and CBP Have Taken Action to Prevent Ineligible Out-of-Country Overstays from Returning to the United States*

In addition to ICE's overstay enforcement activities, in April 2011 we reported that the Department of State and CBP are responsible for, respectively, preventing ineligible violators from obtaining a new visa or being admitted to the country at a port of entry. According to Department of State data, the Department denied about 52,800 nonimmigrant visa applications and about 114,200 immigrant visa applications from fiscal year 2005 through fiscal year 2010 due, at least in part, to applicants having previously been unlawfully present in the United States for more than 180 days, according to statute.<sup>14</sup> Similarly, CBP reported that it refused admission to about 5,000 foreign nationals applying for admission to the United States from fiscal year 2005 through 2010 (an average of about 830 per year) specifically

<sup>13</sup> Verified leads are leads that CTCEU has determined to be accurate and viable by analyzing information from Government and commercial databases containing information related to immigration status. For example, these procedures are intended to verify that an individual suspected of overstaying has not departed the country or been granted an extension of stay by USCIS.

<sup>14</sup> State Department data indicate that a total of about 36.5 million nonimmigrant visas and about 2.7 million immigrant visas were issued from fiscal year 2005 through 2010.

because of the applicants' previous status as unlawfully present in the United States for more than 180 days.<sup>15</sup>

DHS HAS NOT IMPLEMENTED A RELIABLE EXIT SYSTEM AND FACES RELIABILITY ISSUES  
WITH EXISTING VISA OVERSTAY DATA

*DHS Has Not Yet Implemented a Comprehensive Biometric Exit System*

DHS has not yet implemented a comprehensive biometric system to match available information provided by foreign nationals upon their arrival and departure from the United States. In August 2007, we reported that while US-VISIT biometric entry capabilities were operating at air, sea, and land ports of entry, exit capabilities were not, and that DHS did not have a comprehensive plan or a complete schedule for biometric exit implementation.<sup>16</sup> In addition, we reported that DHS continued to propose spending tens of millions of dollars on US-VISIT exit projects that were not well-defined, planned, or justified on the basis of costs, benefits, and risks.<sup>17</sup> Moreover, in November 2009, we reported that DHS had not adopted an integrated approach to scheduling, executing, and tracking the work that needed to be accomplished to deliver a comprehensive exit solution as part of the US-VISIT program. We concluded that, without a master schedule that was integrated and derived in accordance with relevant guidance, DHS could not reliably commit to when and how it would deliver a comprehensive exit solution or adequately monitor and manage its progress toward this end. We recommended that DHS ensure that an integrated master schedule be developed and maintained. DHS concurred and reported, as of July 2011, that the documentation of schedule practices and procedures is on-going, and that an updated schedule standard, management plan, and management process that are compliant with schedule guidelines are under review.

More specifically, with regard to a biometric exit capability at land ports of entry, we reported in December 2006 that US-VISIT officials concluded that, for various reasons, a biometric US-VISIT exit capability could not be implemented without incurring a major impact on land facilities.<sup>18</sup> In December 2009, DHS initiated a land exit pilot to collect departure information from temporary workers traveling through two Arizona land ports of entry. Under this pilot, temporary workers who entered the United States at these ports of entry were required to register their final departure by providing biometric and biographic information at exit kiosks located at the ports of entry. DHS planned to use the results of this pilot to help inform future decisions on the pedestrian component of the long-term land exit component of a comprehensive exit system.

With regard to air and sea ports of entry, in April 2008, DHS announced its intention to implement biometric exit verification at air and sea ports of entry in a Notice of Proposed Rule Making.<sup>19</sup> Under this notice, commercial air and sea carriers would be responsible for developing and deploying the capability to collect biometric information from departing travelers and transmit it to DHS. DHS received comments on the notice and has not yet published a final rule. Subsequent to the rule making notice, on September 30, 2008, the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009, was enacted, which directed DHS to test two scenarios for an air exit solution: (1) Airline collection and transmission of biometric exit data, as proposed in the rulemaking notice and (2) CBP collection of such information at the departure gate.<sup>20</sup> DHS conducted two pilots in 2009, and we reported on them in August 2010. Specifically, we reported that the pilots addressed one statutory requirement for a CBP scenario to collect information on exiting foreign nationals. However, DHS was unable to address the statutory requirement for an airline scenario because no airline was willing to participate. We reported on limitations with the pilots, such as the reported scope and approach of

<sup>15</sup> CBP data indicates that, in total, about 1.3 million foreign nationals were determined to be inadmissible to the United States by the CBP Office of Field Operations from fiscal year 2005 through 2010. As is the case with the State Department, CBP is unable to isolate and quantify the number of aliens it has determined to be inadmissible because of the aliens having overstayed by 180 days or less, because actions taken against these aliens are recorded under grounds of inadmissibility that may apply to, but are not limited to, overstays.

<sup>16</sup> The purpose of US-VISIT is to provide biometric (e.g., fingerprint) identification—through the collection, maintenance, and sharing of biometric and selected biographic data—to authorized DHS and other Federal agencies.

<sup>17</sup> GAO, *Homeland Security: U.S. Visitor and Immigrant Status Program's Longstanding Lack of Strategic Direction and Management Controls Needs to Be Addressed*, GAO-07-1065 (Washington, DC: Aug. 31, 2007).

<sup>18</sup> GAO, *Border Security: US-VISIT Program Faces, Strategic, Operational, and Technological Challenges at Land Ports of Entry*, GAO-07-248 (Washington, DC: Dec. 6, 2006).

<sup>19</sup> 73 Fed. Reg. 22,065 (Apr. 24, 2008).

<sup>20</sup> Pub. L. No. 110-329, 122 Stat. 3574, 3668-70 (2008).



the pilots including limitations not defined in the pilot evaluation plan like suspending exit screening at departure gates to avoid flight delays, that curtailed their ability to inform a decision for a long-term air exit solution and pointed to the need for additional sources of information on air exit's operational impacts.<sup>21</sup> We recommended that the Secretary of Homeland Security identify additional sources of information beyond the pilots, such as comments from the Notice of Proposed Rule Making, to inform an air exit solution decision. DHS agreed with the recommendation and stated that the pilots it conducted would not serve as the sole source of information to inform an air exit solution decision. In July 2011, DHS stated that it continues to examine all options in connection with a final biometric air exit solution and has recently given consideration to using its authority to establish an advisory committee to study and provide recommendations to DHS and Congress on implementing an air exit program.

*More Reliable, Accessible Data Could Improve DHS's Efforts to Identify and Share Information on Overstays*

In the absence of a comprehensive biometric entry and exit system for identifying and tracking overstays, US-VISIT and CTCEU primarily analyze biographic entry and exit data collected at land, air, and sea ports of entry to identify overstays. In April 2011, we reported that DHS's efforts to identify and report on visa overstays were hindered by unreliable data. Specifically, CBP does not inspect travelers exiting the United States through land ports of entry, including collecting their biometric information, and CBP did not provide a standard mechanism for non-immigrants departing the United States through land ports of entry to remit their arrival and departure forms. Nonimmigrants departing the United States through land ports of entry turn in their forms on their own initiative. According to CBP officials, at some ports of entry, CBP provides a box for nonimmigrants to drop off their forms, while at other ports of entry departing nonimmigrants may park their cars, enter the port of entry facility, and provide their forms to a CBP officer. These forms contain information, such as arrival and departure dates, used by DHS to identify overstays. If the benefits outweigh the costs, a mechanism to provide non-immigrants with a way to turn in their arrival and departure forms could help DHS obtain more complete and reliable departure data for identifying overstays. We recommended that the Commissioner of CBP analyze the costs and benefits of developing a standard mechanism for collecting these forms at land ports of entry, and develop a standard mechanism to collect them, to the extent that benefits outweigh the costs. CBP agreed with our recommendation and stated it planned to complete a cost-effective independent evaluation.

Further, we previously reported on weaknesses in DHS processes for collecting departure data, and how these weaknesses impact the determination of overstay rates. The Implementing Recommendations of the 9/11 Commission Act required that DHS certify that a system is in place that can verify the departure of not less than 97 percent of foreign nationals who depart through U.S. airports in order for DHS to expand the Visa Waiver Program.<sup>22</sup> In September 2008, we reported that DHS's methodology for comparing arrivals and departures for the purpose of departure verification would not inform overall or country-specific overstay rates because DHS's methodology did not begin with arrival records to determine if those foreign nationals departed or remained in the United States beyond their authorized periods of admission.<sup>23</sup> Rather, DHS's methodology started with departure records and matched them to arrival records. As a result, DHS's methodology counted overstays who left the country, but did not identify overstays who have not departed the United States and appear to have no intention of leaving. We recommended that DHS explore cost-effective actions necessary to further improve the reliability of overstay data. DHS reported that it is taking steps to improve the accuracy and reliability of the overstay data, by efforts such as continuing to audit carrier performance and work with airlines to improve the accuracy and completeness of data collection. Moreover, by statute, DHS is required to submit an annual report to Congress providing numerical estimates of the number of aliens from each country in each nonimmigrant classification who overstayed an authorized period of admission

<sup>21</sup> GAO, *Homeland Security: US-VISIT Pilot Evaluations Offer Limited Understanding of Air Exit Options*, GAO-10-860 (Washington, DC: Aug. 10, 2010).

<sup>22</sup> 8 U.S.C. § 1187(c)(8).

<sup>23</sup> GAO, *Visa Waiver Program: Actions Are Needed to Improve Management of the Expansion Process, and to Assess and Mitigate Program Risks*, GAO-08-967 (Washington, DC: Sept. 15, 2008).

that expired during the fiscal year prior to the year for which the report is made.<sup>24</sup> DHS officials stated that the Department has not provided Congress annual overstay estimates regularly since 1994 because officials do not have sufficient confidence in the quality of the Department's overstay data—which is maintained and generated by US-VISIT. As a result, DHS officials stated that the Department cannot reliably report overstay rates in accordance with the statute.

In addition, in April 2011 we reported that DHS took several steps to provide its component entities and other Federal agencies with information to identify and take enforcement action on overstays, including creating biometric and biographic lookouts—or electronic alerts—on the records of overstay subjects that are recorded in databases. However, DHS did not create lookouts for the following two categories of overstays: (1) Temporary visitors who were admitted to the United States using nonimmigrant business and pleasure visas and subsequently overstayed by 90 days or less; and (2) suspected in-country overstays who CTCEU deemed not to be a priority for investigation in terms of being most likely to pose a threat to National security or public safety. Broadening the scope of electronic lookouts in Federal information systems could enhance overstay information sharing. In April 2011, we recommended that the Secretary of Homeland Security direct the Commissioner of Customs and Border Protection, the Under Secretary of the National Protection and Programs Directorate, and the Assistant Secretary of Immigration and Customs Enforcement to assess the costs and benefits of creating biometric and biographic lookouts for these two categories of overstays. Agency officials agreed with our recommendation and have actions under way to address it. For example, agency officials stated that they have met to assess the costs and benefits of creating lookouts for those categories of overstays.

#### ADDITIONAL STEPS NEEDED TO ADDRESS RISKS IN THE VISA SECURITY AND VISA WAIVER PROGRAMS

##### *Visa Security Program*

As we reported in March 2011, the Visa Security Program faces several key challenges in implementing operations at overseas posts. For example, we reported that Visa Security Program agents' advising and training of consular officers, as mandated by section 428 of the Homeland Security Act, varied from post to post, and some posts provided no training to consular officers. We contacted consular sections at 13 overseas posts, and officials from 5 of the 13 consular sections we interviewed stated that they had received no training from the Visa Security Program agents in the last year, and none of the agents we interviewed reported providing training on specific security threats. At posts where Visa Security Program agents provided training for consular officers, topics covered included fraudulent documents, immigration law, human smuggling, and interviewing techniques. In March 2011, we recommended that DHS issue guidance requiring Visa Security Program agents to provide training for consular officers as mandated by section 428 of the Homeland Security Act. DHS concurred with our recommendation and has actions under way to address it.

Further, in March 2011 we reported that Visa Security Program agents performed a variety of investigative and administrative functions beyond their visa security responsibilities, including criminal investigations, attaché functions, and regional responsibilities. According to ICE officials, Visa Security Program agents perform non-program functions only after completing their visa security screening and vetting workload. However, both agents and Department of State officials at some posts told us that these other investigative and administrative functions sometimes slowed or limited Visa Security Program agents' visa security-related activities. We recommended that DHS develop a mechanism to track the amount of time spent by Visa Security Program agents on visa security activities and other investigations, in order to determine appropriate staffing levels and resource needs for Visa Security Program operations at posts overseas to ensure visa security operations are not limited. DHS did not concur with our recommendation, stating that ICE currently tracks case investigation hours through its data system, and that adding the metric to the Visa Security Program tracking system would be redundant. However, DHS's response did not address our finding that ICE does not have a mechanism that allows the agency to track the amount of time agents spend on both investigation hours and hours spent on visa security activities. Therefore, we continue to believe the recommendation has merit and should be implemented.

Moreover, we found that ICE's use of 30-day temporary duty assignments to fill Visa Waiver Program positions at posts created challenges and affected continuity

<sup>24</sup> 8 U.S.C. § 1376(b).

of operations at some posts. Consular officers we interviewed at 3 of 13 posts discussed challenges caused by this use of temporary duty agents. The Visa Security Program's 5-year plan also identified recruitment of qualified personnel as a challenge and recommended incentives for Visa Security Program agents as critical to the program's mission, stating, "These assignments present significant attendant lifestyle difficulties. If the mission is to be accomplished, ICE, like State, needs a way to provide incentives for qualified personnel to accept these hardship assignments." However, according to ICE officials, ICE had not provided incentives to facilitate recruitment for hardship posts.<sup>25</sup> ICE officials stated that they have had difficulty attracting agents to Saudi Arabia, and ICE agents at post told us they have little incentive to volunteer for Visa Security Program assignments. Thus, we recommended that DHS develop a plan to provide Visa Security Program coverage at high-risk posts where the possibility of deploying agents may be limited. DHS agreed with our recommendation and is taking steps to implement it.

In addition, ICE developed a plan to expand the Visa Security Program to additional high-risk visa-issuing posts, but ICE had not fully adhered to the plan or kept it up to date. The program's 5-year expansion plan, developed in 2007, identified 14 posts for expansion between 2009 and 2010, but 9 of these locations had not been established at the time of our March 2011 report, and ICE had not updated the plan to reflect the current situation. Furthermore, ICE had not fully addressed remaining visa risk in high-risk posts that did not have a Visa Security Program presence. ICE, with input from the Department of State, developed a list of worldwide visa-issuing posts that are ranked according to visa risk. Although the expansion plan stated that risk analysis is the primary input to Visa Security Program site selection and that the expansion plan represented an effort to address visa risk, ICE had not expanded the Visa Security Program to some high-risk posts. For example, 11 of the top 20 high-risk posts identified by ICE and Department of State were not covered by Visa Security Program at the time of our review. The expansion of the Visa Security Program may be limited by a number of factors—including budget limitations and objections from Department of State officials at some posts—and ICE had not identified possible alternatives that would provide the additional security of Visa Security Program review at those posts that do not have a program presence. In May 2011, we recommended that DHS develop a plan to provide Visa Security Program coverage at high-risk posts where the possibility of deploying agents may be limited. DHS concurred with our recommendation and noted actions under way to address it, such as enhancing information technology systems to allow for screening and reviewing of visa applicants at posts worldwide.

#### *Visa Waiver Program*

As we reported in May 2011, DHS implemented the Electronic System for Travel Authorization (ESTA) to meet a statutory requirement intended to enhance Visa Waiver Program security and took steps to minimize the burden on travelers to the United States added by the new requirement.<sup>26</sup> However, DHS had not fully evaluated security risks related to the small percentage of Visa Waiver Program travelers without verified ESTA approval. DHS developed ESTA to collect passenger data and complete security checks on the data before passengers board a U.S.-bound carrier. DHS requires applicants for Visa Waiver Program travel to submit biographical information and answers to eligibility questions through ESTA prior to travel. Travelers whose ESTA applications are denied can apply for a U.S. visa. In developing and implementing ESTA, DHS took several steps to minimize the burden associated with ESTA use. For example, ESTA reduced the requirement that passengers provide biographical information to DHS officials from every trip to once every 2 years. In addition, because of ESTA, DHS has informed passengers who do not qualify for Visa Waiver Program travel that they need to apply for a visa before they travel to the United States. Moreover, most travel industry officials we interviewed in six Visa Waiver Program countries praised DHS's widespread ESTA outreach efforts, reasonable implementation time frames, and responsiveness to feedback but expressed dissatisfaction over ESTA fees paid by ESTA applicants.<sup>27</sup>

In 2010, airlines complied with the requirement to verify ESTA approval for almost 98 percent of the Visa Waiver Program passengers prior to boarding, but the

<sup>25</sup>The Department of State has designated roughly two-thirds of its 268 overseas posts as hardship posts. Staff working in such locations often encounter harsh environmental and living conditions that can include inadequate medical facilities, limited opportunities for spousal employment, poor schools, high levels of crime, and severe climate.

<sup>26</sup>See 8 U.S.C. § 1187(h)(3).

<sup>27</sup>In September 2010, the U.S. Government began to charge ESTA applicants a \$14 fee when they applied for ESTA approval, including \$10 for the creation of a corporation to promote travel to the United States and \$4 to fund ESTA operations.

remaining 2 percent—about 364,000 travelers—traveled under the Visa Waiver Program without verified ESTA approval. In addition, about 650 of these passengers traveled to the United States with a denied ESTA. As we reported in May 2011, DHS had not yet completed a review of these cases to know to what extent they pose a risk to the program. DHS officials told us that, although there was no official agency plan for monitoring and oversight of ESTA, the ESTA office was undertaking a review of each case of a carrier's boarding a Visa Waiver Program traveler without an approved ESTA application; however, DHS had not established a target date for completing this review. DHS tracked some data on passengers that travel under the Visa Waiver Program without verified ESTA approval but did not track other data that would help officials know the extent to which noncompliance poses a risk to the program. Without a completed analysis of noncompliance with ESTA requirements, DHS was unable to determine the level of risk that noncompliance poses to Visa Waiver Program security and to identify improvements needed to minimize noncompliance. In addition, without analysis of data on travelers who were admitted to the United States without a visa after being denied by ESTA, DHS cannot determine the extent to which ESTA is accurately identifying individuals who should be denied travel under the program. In May 2011, we recommended that DHS establish time frames for the regular review and documentation of cases of Visa Waiver Program passengers traveling to a U.S. port of entry without verified ESTA approval. DHS concurred with our recommendation and committed to establish procedures to review quarterly a representative sample of noncompliant passengers to evaluate, identify, and mitigate potential security risks associated with the ESTA program.

Further, in May 2011 we reported that to meet certain statutory requirements, DHS requires that Visa Waiver Program countries enter into three information-sharing agreements with the United States; however, only half of the countries had fully complied with this requirement and many of the signed agreements have not been implemented.<sup>28</sup> Half of the countries entered into agreements to share watch list information about known or suspected terrorists and to provide access to biographical, biometric, and criminal history data. By contrast, almost all of the 36 Visa Waiver Program countries entered into an agreement to report lost and stolen passports. DHS, with the support of interagency partners, established a compliance schedule requiring the last of the Visa Waiver Program countries to finalize these agreements by June 2012. Although termination from the Visa Waiver Program is one potential consequence for countries not complying with the information-sharing agreement requirement, U.S. officials have described it as undesirable. DHS, in coordination with the Departments of State and Justice, developed measures short of termination that could be applied to countries not meeting their compliance date.

In addition, as of May 2011, DHS had not completed half of the most recent biennial reports on Visa Waiver Program countries' security risks in a timely manner. In 2002, Congress mandated that, at least once every 2 years, DHS evaluate the effect of each country's continued participation in the program on the security, law enforcement, and immigration interests of the United States. The mandate also directed DHS to determine based on the evaluation whether each Visa Waiver Program country's designation should continue or be terminated and to submit a written report on that determination to select Congressional committees.<sup>29</sup> According to officials, DHS assesses, among other things, counterterrorism capabilities and immigration programs. However, DHS had not completed the latest biennial reports for 18 of the 36 Visa Waiver Program countries in a timely manner, and over half of these reports are more than 1 year overdue. Further, in the case of 2 countries, DHS was unable to demonstrate that it had completed reports in the last 4 years. DHS cited a number of reasons for the reporting delays. For example, DHS officials said that they intentionally delayed report completion because they frequently did not receive mandated intelligence assessments in a timely manner and needed to review these before completing Visa Waiver Program country biennial reports. We recommended that DHS take steps to address delays in the biennial country review process so that the mandated country reports can be completed on time. DHS concurred with our recommendation and reported that it would consider process changes to address our concerns with the timeliness of continuing Visa Waiver Program reports.

This concludes my prepared testimony statement. I would be pleased to respond to any questions that Members of the subcommittee may have.

<sup>28</sup> See 8 U.S.C. § 1187(c)(2)(D), (F).

<sup>29</sup> See the Enhanced Border Security and Visa Entry Reform Act of 2002.

Mrs. MILLER. Thank you very much, Mr. Stana. I appreciate all the testimony of all the witnesses. I know we have a lot of questions.

One of the things that struck me as you all were testifying was the common theme about sharing information, et cetera, and working together with your sister agencies, with your partners and having good partnerships. That is a theme in my office and I think certainly most Members' offices, that was a critical element of the 9/11 Commission recommendations about moving from the need to know to the need to share and getting out of our respective silos, et cetera, et cetera. We talk about that all the time. It is very important certainly. I think that is why our committee staff put you all so close together. You are just smashed together.

As I mentioned, the first and foremost responsibility of the Federal Government to provide for the common defense is actually in the Constitution; securing our borders is a Constitutional mandate of the Congress, and that is what this committee is all about. So we want to work with the administration in every way possible to secure our borders. I really do not look at it as a Republican or Democratic issue. I see this in very nonpartisan terms. I am delighted that because this committee has been very, very vocal about continuing the presence of the National Guard as a force multiplier for CBP and Border Patrol along the Southern border the administration just recently has agreed to do so for some period of time. I think we could use more, but still it is a very, very excellent, positive step forward, I think.

Mr. Cohen, as you are outlining today, I don't know whether serendipity or whatever, you don't need to comment on that, but certainly the timing of having the administration talk about things that this committee has been pushing for for some period of time in regards to the visa program, announcing those today as we are having this hearing does strike me as a bit interesting and very welcome, very welcome. So we are delighted to hear about those kinds of things.

I guess I would start, Mr. Cohen, with you. I was trying to take some notes as you were outlining this. So there may be a couple of questions in this. But you mentioned that you had 1.6 million names that you started with and about 800,000 of those you found then had left, which was an interesting number. So we really didn't know about that until you started this, which is okay, and then 839,000 left to vet, which you have done so, several thousand sent to ICE. I am trying to understand where we are in this whole vetting process, if you would flesh out your testimony a little bit with that, because you mentioned also that Congress would get the data for instance by country and some of the other metrics that you outlined. I am interested to know when that might be. I thought you said 6, 12 months. I am interested in that.

I guess just generally there is no secret about the painful economic transition that is happening Nationally and all of us are concerned about the budget deficit, and what we want to do of course is prioritize our expenditures so that we are doing what we need to do with the resources that we have. I think by using technology—that was going to be a question I had before you outlined here about the biometric forms, and some of the biometric and bio-

graphic information, of course using the biographic information, but the biometric forms whether that is iris scan or retinal scanning or fingerprints, all of these different kinds of things. I am a big believer in utilizing technology as a cost-effective, cost-efficient, in this case National security efficiency matrix as well has been overlaid. So I was delighted to hear you talk about that.

So I don't know if I am making my question clear, but I am trying to understand exactly what it is that you have outlined for us today, because what you said is essentially what we have been trying to get at as a committee.

Mr. COHEN. Thank you, Madam Chairwoman. I think you are right, there are a couple of factors that have come into play that have allowed us to come here today and be able to describe what I think is a pretty fully based approach to how to deal with this issue. I think the level of cooperation that has matured across not only the Department, but across the Federal interagencies, across the law enforcement community, the intelligence community as well as the immigration community, coupled with quite frankly a maturation of information systems. Whether it is the information systems of the NCTC, the information systems of the intelligence community, the information systems used by US-VISIT, ICE, and CBP and State Department, there has been a maturation over the last several years. I would argue that what I started to describe earlier probably could not have occurred several years ago.

So how do we get to where we are today? Earlier this year, for many of the reasons you all have outlined earlier, the Secretary pulled CBP, ICE, US-VISIT together and said, we need to vet the 1.6 million records that are commonly referred to as the overstay backlog from a National security and public safety perspective. We have to get it done and we have to get it done now. That meant we all came together and we reached out to our intelligence community colleagues and we came up with a way to leverage existing technical capabilities to vet from a public safety and National security perspective those records.

The first step was US-VISIT running through their systems that 1.6 million records. That is how they were able to eliminate the first tranche of that data to determine that they had left the country or they had actually changed their immigration status.

The remaining records, a portion of those were considered confirmed potential overstays. Based on existing protocols those 82,000 records would have been more fully evaluated under the pre-existing manual database checks and protocols that existed through the ICE prioritization process.

What we did this time is we took those 82,000 records and the remaining 757,000 records, which under the prior paradigm would never have been fully vetted, and we ran them through the NCTC system and then we then leveraged the capabilities of automated targeting system to query not only law enforcement and other immigration databases but we leveraged the intelligence-driven targeting rules that ICE—that CBP utilizes in the course of their general business. Out of 839,000 records we were able to identify a subset that were potentially public safety or National security threats. Working with ICE and CBP and the intelligence commu-

nity, we were able to essentially go through each and every one of those 2,000 records.

A subset of those, several hundred, were potential leads that ICE eventually ran down to the point where we were talking about dozens. So we started with 1.6 million records and ended up with dozens of new investigations. Now some of those, several hundred, were preexisting investigations, some had died, some were in jail. Which think they were overstays because they were actually in jail. Some we determined had left the country because we were querying different databases like Interpol databases, et cetera. But we were able to automate that public safety and national security vetting process.

We brought the same group together to say, okay, can we do the same thing from a location and immigration status perspective? Current capabilities did not allow that. To be able to vet those 757,000 records from a location and immigration status perspective would have required time-consuming manual databases—database queries, excuse me. So we put this team—we focused this team on coming up with a design on how to automate those processes as well. That work has been underway for several months now. I think we have come up with a concrete plan. As we looked at what would result when we put that plan into motion, we estimate will take between 6 to 12 months, we will have phased in results along that time period. We not only will be able to fully vet from an ongoing basis any other potential overstays, or visa applicants, or visa holders, or people requesting other immigration benefits from a public safety or National security perspective, but we will also have enhanced biographic exit capability from added biometric features, such as better utilization of fingerprint identification numbers and other biometrics. If we couple that with research being done by our S&T on biometric data collection capabilities from an exit perspective, you have the foundation for a biometric exit capability in the future.

Mrs. MILLER. Well, I for one cannot tell you how much better I feel now than I did at the beginning of this hearing listening to your explanation and as you have been talking about your process here. I guess one follow-up, when you talk about follow-on, sometimes “follow up” are the two most important words in the English language. You have this large group that you began with, 1.6 million, and you went through various iterations down to a couple of hundred apparently that are continuing with some sort of investigative process there. How will you do in following up so we never get to that huge backup again? So you will be able to—maybe you told me that, but I didn’t quite get it. How are you going to continue to do this so it will not happen in the future, we will be able to in real time understand if there is a significant threat to National security—not 6 months after the fact.

Mr. COHEN. So, for me, one of the most exciting parts of this has been to watch how as we have brought more clarity to the technological capabilities that can come when we interlink these systems, that that has caused a parallel excitement on the operational side. ICE has, working with CBP and others, has been rethinking the way that they track day-to-day. So instead of us being reactive, an overstay list being—a potential overstay list being created, it being

prioritized best based on preexisting prioritization standards, CBP and the technologists will be working developing essentially a hot sheet, which on day-to-day will look at new derogatory information coming in, new immigration information coming in, new travel information coming in and will essentially create a dashboard available to ICE on a day-to-day basis that will provide them insights about those public safety and National security risks that are either overstays or existing visa holders.

So ICE is actually—this has provided an opportunity for ICE, as they are able to free up more personnel from these database queries, to be more imaginative and creative in how they use their existing investigative resources.

Maybe I would defer to Mr. Edge if he wants to add any more to that.

Mrs. MILLER. Mr. Edge.

Mr. EDGE. Thank you very much, Chairwoman Miller.

That is certainly a very accurate assessment. The part that US-VISIT begins we are able to take after all these leads have been fully evaluated and vetted through various databases, and then we farm those leads out to our various offices in the field. We have 265 offices on the domestic side and 70 offices internationally. So once those leads are sent out to the field, our agents are able to conduct investigations and very detailed investigations, based on the quality of the information that we have received.

So it certainly has worked very well. We certainly see that it is going to continue to work. We also have received well over 194,000 leads, not only from US-VISIT, but from the SEVIS process as well. We have initiated 7,272 investigations as a result, and that is pretty significant, certainly something that we haven't been doing over the past—since the inception of the agency and us trying to combat terrorism.

As a result, we have also been able to make 2,194 arrests. So the information that we are getting now has really been analyzed carefully, resulting in some significant results. As Mr. Cohen indicated, we are able to conduct some quality investigations by gathering this information and sending it to additional databases in the intelligence community as well as our counterparts in the law enforcement world.

Mrs. MILLER. Thank you very much.

I would just conclude my questioning here by once again observing that this is really how Congress is supposed to act, where we are doing oversight, we are asking various questions, hopefully getting the agencies to respond.

You certainly are responding and I think in a very appropriate manner. So I am appreciative to hear all of this today.

With that, I would like to recognize our Ranking Member, Mr. Cuellar, for his questions.

Mr. CUELLAR. Thank you very much, Chairwoman.

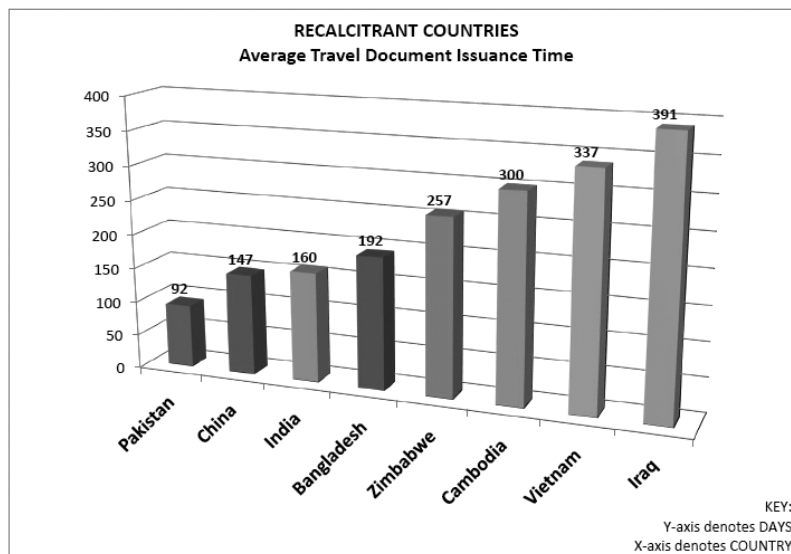
I have two sets of questions. One has to do with the time that after an alien is ordered to be removed, how long it takes for that person to stay.

Members, I would ask you to look at the handouts, and I believe Diana is going to put an overhead also. What is the average time



to get the travel documents issuance before they are removed? So it involves a little bit of the State Department.

[The information follows:]



Prepared by the Office of Congressman Henry Cuellar

The other one is an issue I brought up at the committee last week, I believe, about a Mexican-based school that taught students how to fly. They were in south Texas. Instead of being there on student visas, they were there learning—being taught on tourist visas it sells. Again, the way this came about, because one of the Mexican pilots, training pilots, went over and buzzed some of the boats at one of the places and had to create that type of activity to bring this up.

So I will go first with the travel. As you know, when an alien other than a Mexican national is ordered removed from the United States, a consular officer from the alien's country of origin must issue a travel document. This travel document allows the alien to return to his or her country and are necessary to effect the order removal of aliens from the United States. There are some countries, like Guatemala, Honduras, and the DR that have electronic travel documents that make that to move a lot faster. Of course, with Mexico overall we have a good working relationship where they will take them rather quickly.

But as you can see up there, there are certain countries, and this is only just a few: Pakistan takes 92 days. This is after—just to get the travel documents. China, 147 days; India, 160 days; Bangladesh, 192 days; Zimbabwe, 257; Cambodia, 300 days; Vietnam, 337; Iraq, 391 days. Again, I know from the State Department, because—and I want to thank John Morton, because he is the one that brought up this issue about a year ago. We sat down with the

State Department, and we were given the diplomatic reasons why the State Department couldn't move on.

But at the same time, keep in mind that that will cost us money, because any time they stay here in the United States, it is going to cost us money. This is from the time an order was given. This is not before the time; this is after. So if you add all of those, it is going to cost the taxpayers thousands and thousands and thousands of dollars to keep those folks here.

The chart, as I mentioned, those are the recalcitrant countries that are just slow in accepting their nationals back, and they will give up different reasons. They are good at giving information so they can get their visas. But when we want to send them back, they will give you all these reasons.

My only thing is this: If we can be given the reasons again why it is difficult to get these countries to get them to accept the folks back and what is being done by the United States, and are those delays a consideration when determining whether to issue visas to individuals for certain countries? My thing is, if they are taking a hard time to take back those folks, then when we give them visas, why are we continuing to give them visas when at the end, they are going to take their time? I really think that the State Department should consider that. Should we consider restricting visa issuance to those countries until they begin to accept their nationals in more timely visas? Again, I am a Georgetown Graduate School of Foreign Service, I understand all the diplomatic reasons. But again, as a taxpayer and as a Member of Congress that represents all those folks, I think that is something that we need to play a little bit more hardball with those countries that are taking their time and costing us a lot of money.

The second part of the question is the situation that we had in south Texas. How can students that come in, take flying lessons in small planes—and we know what happened in 9/11. You know they are coming in to learn. They are here on tourist visas and not student visas. Then of course, when we talk to the FAA and Homeland Security, everybody will say, well, we don't do this, we don't do this, we don't do that. That is their responsibility, not our responsibility. It goes to what the Chairwoman and Chairman Thompson has been and all of us have been talking about, all Members of the committee, is: Where is the coordination?

I mean, at the end of the day, the American taxpayer doesn't want to know what agencies blame what agency. They want to know: What are the results and how are you keeping us safe? The first part of the question is the recalcitrant agent countries. I guess we will start with the State Department.

Mr. RAMOTOWSKI. Thank you, Congressman.

Let me first say that the State Department is acutely aware of the seriousness of this issue. We share your concern. We are taking all possible steps to improve the situation with respect to recalcitrant countries. Together with our interagency partners we have established a high-level working group to work out a strategy for dealing with the most egregious countries. In addition to that, former Under Secretary Burns, now deputy secretary, instructed all our chiefs of mission to do what they could to produce positive responses in the recalcitrant countries.

Mr. CUELLAR. Could I ask you a question? Since April—I think it was in April 2011 that we met in my office with the State Department and John Morton. Has anything been done except establish a working task force—with all due respect. I mean that with all respect. I appreciate all the help that you and Secretary Clinton are doing. Anything been done since that time besides incur more taxpayers' dollars? Is the task force the only thing that has been done?

Mr. RAMOTOWSKI. Well, these issues are also being addressed case by case with the foreign consulate officers here in Washington. Again, our staff works with ICE and the other agencies involved to try to encourage the foreign countries to take back more of these individuals. But as you have recognized, it is a difficult process. There are many issues at stake, and the progress hasn't been as rapid as we would all like.

I would point out, too, that our new ambassador to China, former Secretary of Commerce Gary Locke, is personally aware of and engaged in this issue and is determined to see more progress with respect to China. So we are doing everything that we can. Let me close by saying that for us, this is a very serious issue.

Mr. CUELLAR. I appreciate that. Could we put a little bit more pressure on them at the beginning instead of the end?

Mr. RAMOTOWSKI. We will try our best, sir.

Mr. CUELLAR. We will follow up on the second question on the second round on that. Just keep thinking about that particular case in south Texas.

Thank you, Madam Chairwoman.

Mrs. MILLER. I thank the gentleman.

The Chairwoman now recognizes the other gentleman from Texas, Mr. McCaul.

Mr. MCCAUL. Thank you, Madam Chairwoman.

Fifteen of the hijackers came from Saudi Arabia. When I look at the Visa Security Program, it does not have 11 of the top 20 high-risk posts included, including Saudi Arabia, which seems sort of interesting to me.

So Mr. Edge and Mr. Cohen, can you explain to me why Saudi Arabia is not on this—part of this program?

Mr. EDGE. I believe Saudi Arabia is a part of the program as we speak today.

Mr. MCCAUL. They are?

Mr. EDGE. Yes, they are.

Mr. MCCAUL. Then perhaps I had some misinformation.

Let me continue with Mr. Cohen. I am glad that after 10 years later, we are making progress on our exit program. When do you plan to have that fully implemented?

Mr. COHEN. We anticipate that the capabilities that I described earlier will be implemented within 6 to 12 months.

Mr. MCCAUL. Will that include also biometric?

Mr. COHEN. It will include enhanced biographic with certain biometric elements included. As I referenced earlier, more expanded use of information captured on the front end, fingerprints, et cetera. We are also—it will also include within that same time period more advancements in research on biometric technologies we can use here as part of the exit program.

Mr. MCCAUL. I agree with Madam Chairwoman. That is certainly good news. That is where the Congress in our oversight working with you actually is a positive experience.

Let me move on to visa overstays. The Secretary announced that criminal aliens are a high priority for deportation. As a former Federal prosecutor, I certainly understand that with limited resources. On the other hand, she seemed to infer that noncriminal aliens that were having visa overstays could stay in this country and apply for work permits.

First of all, Mr. Edge, can you respond to that; is that the administration's position?

Mr. EDGE. Well, our position as a law enforcement agency is to take the information that we acquire from the SEVIS program and US-VISIT and focus on those overstays that pose the most threat and potentially are the most dangerous to our country.

Mr. MCCAUL. I get that, and I agree with that. But I was disturbed by the inference that the noncriminal aliens overstaying could stay here and apply for work permits. Was that an accurate statement on the part of this administration?

Mr. EDGE. I am not familiar with that statement. I would have to defer to the Department.

Mr. MCCAUL. Okay. Perhaps I need to ask the Secretary herself that question.

Mr. STANA, if that is the policy of this administration, do you think that would pose a threat in any way to our security?

Mr. STANA. Well, given with the theme of the hearing, the integrity of the visa process, you would certainly call it into question.

Listening to the new program that ICE and DHS is putting together, I think it is a step in the—I would welcome the opportunity to take a look at it. It raises a whole host of questions. But if we are still going to focus on the National security and public safety folks, which is the thing to start with, it still leaves the vast majority of people untouched, and it gives the impression that once you are in the country, you are in, unless you act out, and then you might get caught.

Mr. MCCAUL. Because as I look at some of these, whether it is hijackers or high-profile terrorist violators, many of them were non-criminal aliens here on a visa overstay.

Mr. STANA. Well, and the fact that the Christmas day bomber went through the visa processes, many of which were in place in December 2009, apparently got in on the airplane and got a visa, just calls into question how much question has to be raised before you deny boarding.

Mr. MCCAUL. Mr. Edge, I hope you can get back to me on that question in terms of what is the administration's position.

[The information follows:]

A typical scenario is someone enters legally, overstays, marries a United States Citizen and applies for adjustment of status. I believe in this case the person may qualify for an Employment Authorization Document (EAD) based on the pending I-485, *Application to Adjust Status*. Here are some other examples under which an individual, like an overstay, would get an EAD:

- Deferred Action;
- Temporary Protected Status;
- Withholding of Removal;
- Applicant for Cancellation of Removal;

- Certain Asylum applicants (where applications have been pending for more than 180 days);
- Certain individuals who are subject to Final Removal Orders can also apply for employment authorization if they cannot be physically removed for some reason or if they are the sole supporters of other family members.

[Ruth Tintary, Associate Chief Legislative Branch for USCIS provided this answer to ICE, Office of Congressional Relations]

Mr. McCAUL. Or perhaps, Mr. Cohen, you may have an answer to that.

Mr. COHEN. Yes, Congressman, if I may.

So, first and foremost, because of resource issues primarily, the administration prioritizes the targeting of those visa overstays that represent a National security or public safety risk. Through the capabilities that I have described earlier, as we are better able to identify people who are actually confirmed overstays, meaning we have assessed that they are actually located in this country and they have not changed their immigration status, we then, as we do now, will have the ability to provide that information so they can be inputted by CBP and others into their systems and State Department into their systems. So if there is a second encounter, meaning they are arrested, meaning that they seek to apply for another visa, they seek to apply for other types of entry, the information that they are an overstay will be available to those CBP officers or others.

Mr. McCAUL. Well, again, a majority of the hijackers were overstay noncriminal aliens. The Blind Sheik responsible for the 1993 World Trade Center bombing was a visa overstay without a criminal record. So I think it is important, and I am concerned—and that is why I look forward to hearing from the administration—I am concerned about sending a message out there that if you are a noncriminal alien, it is okay to stay; in fact, you can apply for a work permit as well.

Mr. COHEN. If I may, Congressman, one last point. You make an excellent point about whether information about the hijackers was in databases like NCIC because they have been arrested. What there was on many of the hijackers, or on several hijackers, was derogatory information or other law enforcement information that under this new construct would come to the attention of authorities; information in FinCEN, information that may reside in other repositories of the intelligence community, other than say the TSDB. So what we are seeking to do is expand our ability to vet visa information or information regarding potential overstays against a much broader set of law enforcement or intelligence information than we have done so in the past.

Mr. McCAUL. I look forward to working with you on that, and thank you for your testimony.

Mrs. MILLER. Thank you.

The Chairwoman now recognizes the gentleman from Virginia, Mr. Rigell.

Mr. RIGELL. Thank you, Madam Chairwoman.

Thank you all to our panel. I appreciate the work that you are doing.

You know, that we have had no major domestic terrorist attack since 9/11 certainly is a high degree of success, and we recognize that. Now, also, though, at the same time that we have approxi-

mately 4.5 million illegal immigrants here who came here on a visa and then overstayed, that is unquestionably a failure. I am going to in my short time here try to see how we link performance with—and accountability with performance here.

Mr. Ramotowski—I, too, have a difficult last name to pronounce—what is the approximate number of countries whose citizens are eligible to apply for a visa to come to the United States?

Mr. RAMOTOWSKI. Well, the citizens of all countries are eligible to apply to travel to the United States.

Mr. RIGELL. Okay. So any country?

Mr. RAMOTOWSKI. Yes.

Mr. RIGELL. Now, among that range of countries then, surely there is some disparity between those countries whose citizens have a higher percentage of violating our visa conditions than others, right?

Mr. RAMOTOWSKI. That is correct.

Mr. RIGELL. Okay. Could you please identify for us then those top five countries?

Mr. RAMOTOWSKI. I don't have statistics here, sir, on the number of visa overstays by country. We would have to get back to you on that.

Mr. RIGELL. Okay. If you would, please. Not so much by the—well, I would like it to be the actual number, but also as a rate, a percentage. Because those countries who—it would indicate to me that if we have the top five countries, I would say, what is taking place at our offices there, our State Department offices there, our embassies, to understand what is taking place there?

Now, on that, as a follow up, with the actual personnel side, actually approving a visa is by definition a judgment call. We are trying to predict future human behavior, inherently difficult. We have some mechanisms that help us with that and the biometrics that we are working on, on all of those things, but at the end of the day, it is a judgment call. It would stand to reason, wouldn't it, that some folks are better at that than others, wouldn't it?

Mr. RAMOTOWSKI. That is correct.

Mr. RIGELL. Okay. What processes and procedures do we have in place that would help us discriminate in the most positive sense of the word those personnel who are really good at this and others who clearly aren't very good at it?

Mr. RAMOTOWSKI. Well, again, Congressman, we have a layered approach to the training of our personnel. As I mentioned in my statement, they receive an intensive basic consular course when they join the Foreign Service that includes training in interview techniques, behavior detection and all of our consular automated systems. Many of them also do consultations with other law enforcement agencies before they go out to their post. When they arrive in country—and I should also point out that they are given training in the language and culture and area studies of the regions to which they are sent. When they arrive in country, senior consular personnel are charged with overseeing their professional development and monitoring their work.

Mr. RIGELL. I appreciate that.

I really don't want to be rude by interrupting you. We have such little time here, and this is a very important question for me. Let's

say, for example, that there are 500 visas approved by a particular person and their failure rate is in the 12 percent range, and generally, you would say, well, that is pretty good compared to maybe the average for that country. But there is another person over time who you see has a 42 percent failure rate, that is 42 percent of the visas he or she approves actually end up overstaying. I am trying to—I am trying to help our Government have this culture of accountability. So you have described a lot of things there, but I did not hear how we circle back around and try to track performance, not to punish someone, but to help those—to elevate those who are doing well, and maybe if we do have a person who is not having a particularly good track record on this, that we either help them become better or, frankly, we remove them.

Mr. RAMOTOWSKI. Well, Congressman, as I was saying, we do have a process for evaluating our personnel. It is a continuous process. Individuals who do not perform to the Service's expectations can be denied tenure and removed from Service.

Mr. RIGELL. Thank you, sir. I just would circle back maybe around on some written questions that I will submit to understand better the metrics of that, if there are actual metrics of violations.

Thank you, Madam Chairwoman.

Mrs. MILLER. Thank the gentleman.

The Chairwoman will now recognize the gentleman from Florida, Mr. Bilirakis.

Mr. BILIRAKIS. Thank you, Madam Chairwoman.

I appreciate you giving me the opportunity to participate today.

According to the Homeland Security Department's numbers, more than 7,300 foreign students have left school early for various reasons but illegally remain in the United States. More than 800,000 students in the United States participate in the Student and Exchange Visitor Program. Most of them come here for noble intentions. While not all would-be terrorists come to the United States under the guise of a student visa, we have seen examples where several have. I know everyone—well, we have examples right here.

For this reason, I have long advocated for legislation of the Student Visa Security Improvement Act, which I introduced to ensure that student visas are issued to those genuinely interested in obtaining an education. It seeks to ensure that once allowed into the country on a student visa, students are actually here to study and do not drop off the radar. So I have a couple of questions here.

Secretary Ramotowski, to what extent does the State Department coordinate with DHS to review and screen student applications for security concerns?

Mr. RAMOTOWSKI. Congressman, student visa applicants are screened through the same intensive process that all these applicants are screened with, with some additional features. They have their fingerprints taken and screened through our biometric fingerprint systems. We also use facial recognition technology to screen those applicants. We conduct an intensive visa interview with consular officers in the local language or in English. In addition to that, we utilize extensively the Immigration and Customs Enforcement SEVIS system to ensure that the student is attending a reg-

istered school and has in fact completed the registration process at that school.

As I mentioned in my remarks, after the visa is issued, there is a continuous vetting process of all issued visas, such that if at any time derogatory information surfaces from any source, law enforcement or intelligence, it can be promptly analyzed and the visa can be reviewed for possible revocation. So, yes, we work very closely with Homeland Security and our other partner agencies on these cases.

Mr. BILIRAKIS. Well, why is it then that we have 7,300 students that are here—or former students that are here illegally in the United States? How can we help you with that issue?

Mr. RAMOTOWSKI. I think, Congressman, and I obviously can't speak for them, but individuals overstay for a variety of reasons. We are continually reviewing our processes at our posts abroad to ensure that if there is a change in the country, perhaps economic activity, an economic crisis or something of that sort, that our officers are fully aware when they make their visa adjudication decisions that there might be other factors encroaching on an individual's decision whether to comply with our immigration laws or not. We will never knowingly issue anyone who is unqualified or has an intention to overstay in the United States a visa.

Mr. BILIRAKIS. Are we searching for those individuals, those 7,300, that are located here in the United States? Do we have any idea where they are?

Mr. RAMOTOWSKI. I will defer to my Homeland Security colleagues on that one.

Mr. EDGE. If I may, Congressman, ICE is working very closely with the Department of State in sharing our various databases. Currently we have more than 10,364 institutions as a part of the SEVP program, and we follow up with the various institutions on a regular basis to determine if these students are remaining in school. So those students that certainly are out there as overstays, their names are being vetted through the various systems that we highlighted earlier in our testimony today, and they are being prioritized. We certainly would be looking for the most egregious ones, those that pose a threat to our National security.

Mr. BILIRAKIS. Thank you.

For the entire panel, to what extent are some fraudulent educational institutions able to serve as visa mills and as a back door into the country? What tools exist or are needed to close this loophole, for the entire panel?

Mr. STANA. Well, I will start off. I think what my other panelists said was probably what we all wish for. We all hope that the information provided by the educational institutions is accurate and there is no fraud. Our work has shown, however, that that is just not the case. Sometimes information which ICE depends on to do its casework is submitted late into SEVIS or not at all. The students themselves don't update the information that they have to update about their job status, so it may appear that they are still in school.

There is fraud involved, Mr. Bilirakis. I think you mentioned that is what you alluding to, at universities. There was one in the paper I think, and I am not saying this was fraudulent, but Uni-



versity of Northern Virginia, that was alleged to be of the type that you are saying.

So I think that we have to take more steps than we have in the past to make sure that this is as seamless as we would like it to be. Right now it is not. There are too many inaccuracies in the data, and there are too many cases of fraud in connection with these schools, other people taking the students' tests for them, people not checking photo IDs when they should, and so on.

Mr. RAMOTOWSKI. I would just like to add, Congressman, that that underlines the importance of the personal interview that our officers conduct and our embassies and consulates. Because although someone may submit a fraudulent test paper, a highly trained consular officer can often note discrepancies in the interview that would open a line of inquiry and lead to the denial of that visa.

In our high-fraud posts, we also have fraud prevention units and fraud prevention managers. They are dedicated to ensuring the integrity of the visa system. They investigate questionable cases and provide the results of those investigations back to the visa officers. So we take this concern very seriously, and we work closely, again, with Homeland Security in maintaining the integrity of the process.

Mr. BILIRAKIS. Madam Chairwoman, I know my time has expired. I have one additional question, but I will wait for the second round.

Mrs. MILLER. Okay. Thank the gentleman.

The Chairwoman now recognizes the gentleman from South Carolina, Mr. Duncan.

Mr. DUNCAN. Thank you, Madam Chairwoman, and thank you for the timeliness of this hearing.

It never ceases to amaze me that when we schedule a hearing on a topic like this, that we see the administration react in a positive manner, and then that is a good thing.

There was an article today in the AP, "Broader Security Checks to Reduce Visa Overstays." It may have been brought up earlier, but it is a good thing that we are having an impact, so thank you for that.

I want to address my question, I guess it could go to Mr. Edge or Mr. Cohen or Mr. Stana, but visa overstay is definitely a topic that concerns folks in my home State of South Carolina, because we know that we have got to do a better job than what we do in this country. When you see statistics, such as a backlog of 1.6 million people have overstayed their visas in the United States—and recently you all have vetted those through multiple channels, which I will talk about in a minute, there are still 839,000 people here that I think Mr. Cohen said the Department vetted everyone for potential National security and public safety concerns. But there are still 839,000 people here that have overstayed their visa in violation of the sovereignty of the United States of America, and I just have to say, why? Why do we still have 839,000 people here who are here illegally?

Mr. COHEN. Great question, Congressman, and you have made a really important point.

The sad fact is that we do not know until we go through a manual vetting process what number of that 839,000 actually are either still in this country or have changed immigration status. That is why the capabilities I described earlier are so important, because in the past, because of resource issues and the lack of technical capability, it required US-VISIT, ICE, to manually do a series of manual database checks that was incredibly time-consuming, so there were large numbers of records that were never evaluated. Now, those people may have left. They may have changed status; we just did not know that.

Mr. DUNCAN. Can you pause right there and explain to me as a freshman Congressman what “change in status” is, what you mean by that?

Mr. COHEN. Change of status means they came into the country under a visa, they may have changed their immigration status. They may have extended their visa. They may have reapplied for a new visa. They may have applied for a new visa with a slight variant in their name.

Mr. DUNCAN. Would not we know if they applied for a change in status that they are no longer here as a student and they have changed and you take them out of that category, wouldn't that be automatic?

Mr. COHEN. In some cases, yes. In some cases, the way that the systems had been designed in years past, that information was not immediately apparent, and it would require an individual, an investigator, or a researcher, to go into multiple systems to determine that.

Mr. DUNCAN. So if Tom Davis comes into this country from Ireland and he realizes he is here on a student visa, he overstays his visa, he has gotten a job or he is now consulting for a company, and he wants to change that status to here for business reasons or whatever, and he comes to your office and says, I want to change my immigration status, Tom Davis from Ireland, here is my Social Security Number, here is my whatever identifying factor that you have, you can't electronically with all the abilities we have today take that Tom Davis out of that category and put him in another, and he would not be listed in the 839,000 people that we are talking about now? Is that that difficult?

Mr. COHEN. The way systems were designed in the past, yes, sir, and that is what we are fixing.

There is one example I can talk to you about the 839,000 records that we did vet, where we found an individual who came based on a visa applied for by her husband. She then changed status and got a visa on her own. She is a very good student at a southern university. The system would not have automatically picked that up and did not. That is what we will be fixing through this new capability, this interlinking of systems that I referred to earlier, Congressman.

Mr. DUNCAN. It is very obvious to me that we have got a broken visa system for overstays based on these numbers when you vetted over half of them through multiple channels and said, okay, those guys have gone back to their country; we still have 839,000, 2,000 of which warrant further investigation because they are probably here for maybe God knows what. But I believe that we have got to pursue in this Nation, in my last seconds here, a biometric coun-

tercheck so that we know when someone leaves this country that they have left. If they haven't shown up and left the country within their stated time, then we put them in a category that they are here illegally and we start running down their last address and we start taking care of securing our country.

The sovereignty of this Nation is very, very important to me. It is no wonder we see instances like we recently saw with a member of a certain family who has been here, overstayed a visa for a very, very long time, so very timely. Thank you.

I yield back.

Mrs. MILLER. I thank the gentleman for those comments.

I think the gentleman has demonstrated a frustration that many of us feel that when you see an administration who has just recently announced their policy that say they are not going to deport illegal aliens, known illegal aliens, unless they think they are a public safety threat.

So that is a very unfortunate backdoor amnesty, however you want to characterize. It is an end-run around the legislative process.

I am now speaking to other Members of Congress. I don't expect any comment from any of our panelists. I am talking about an administration-announced policy that I have vehemently stated I have a lot of problems with. I think that is going to add to our problem. It is going to incentivize others to get here, stay here, and knowing that unless they really do something criminal, even a DUI, which apparently is not enough criminal activity to be a public safety threat to deport an individual. That is a significant problem I believe to our National security here and to the political will of the American people who have demonstrated over and over again they want to secure our borders and they want to get rid of a lot of the illegal aliens who are here, whether they are overstays or what have you.

I would just comment to Mr. Stana, because you have mentioned here—one thing that you said that I felt was very interesting, when you said the amount of the budget that we are spending to protect, secure our borders and yet here we have 40 percent plus of all the illegals that are in the country are overstays from their visa. You just mentioned specifically with ICE that you are only spending 3 percent of your budget on these overstays when they are 47 percent of some of the problems that we have.

So I would just ask Mr. Stana, you mentioned about the information Mr. Cohen gave today and you looking forward to evaluating that. Will the GAO just go ahead and evaluate this? Or are you looking for a letter from our subcommittee, or what will trigger your analysis and recommendation?

Mr. STANA. What would trigger a study would be a letter from the subcommittee or committee.

Mrs. MILLER. You are going to have it very shortly then.

Mr. STANA. If both sides would do it, it would be advantageous.

There are a number of questions that were raised. I think this is definitely a step in the right direction, but there are questions about timeliness and reliability when you are using biographic versus biometric. The rest of the system has to be resourced to be able to move people along the line to deportation, if that is the

goal. Of course, you mentioned the immigration impact aside from the National security impact, and when that part of the tail would be resourced as well. So there are lots of questions. As I say, it is a step in the right direction. It is something that I am sure you have been looking for for awhile. I just would like to see how reliable the system would be.

Mrs. MILLER. Very good. That letter will be forthcoming.

I also want to mention again about the Christmas day bomber. Obviously, I come from southeast Michigan. That particular incident has sort of faded from the National radar screen, but I will tell you, it has not faded in my media market, because as we speak, the Christmas day bomber, who is now his own attorney, he is his own attorney, and they are going through jury selection. It makes me crazy every day I am watching this guy going—after we Mirandized him, sent him to the University of Michigan, the best burn center in the entire Nation, and now he is going through this entire process, and how much the city of Detroit actually is having to pay for security, et cetera, for this guy going through our system when he should be, in my opinion—again I am talking to other Members of Congress; I am not looking for any comment from any of you, this is an administrative-stated policy—this individual in my estimation should be treated as an enemy combatant. They are looking at the battlefield in asymmetrical terms, and on that particular day, the battlefield was seat 19A of that Northwest flight, and that was a battlefield in his mind.

I think we hurt ourselves by not appropriately responding to that. But I guess this is a question in regards to him, because it is my understanding that running the name through the NCIC database, et cetera, that his name as it was introduced after his father came to the embassy in Nigeria, et cetera, was misspelled. So how has that—I mean, will that happen again? What steps have we taken to correct that?

Mr. RAMOTOWSKI. Madam Chairwoman, we have taken a number of steps to ensure that that will never happen again. The database that we use to store the records for issued visas has fuzzy logic for name searches such that a future search, a current search with a misspelling will still return all possible records and close matches. In addition to that, our embassy in Nigeria had forwarded a telegram, as was noted here, to Washington indicating that the father had come in and had concerns about his son's dealings with extremists in Yemen. That was sent as a Visas Viper message. At that time, the interagency watch listing guidance did not call for the automatic watch listing of that sort of information. That has been changed, and at this point, I have no doubt whatsoever that Mr. Abdulmutallab would have been watch listed, would be watch listed now. The State Department in turn has changed its revocation policy. Upon receipt of a Visas Viper message of that kind now, we automatically review the issued visa for revocation and act upon it, unless a law enforcement or intelligence agency has formally asked us not to take action.

So we have corrected many—all of the State Department issues that were identified in the aftermath of the Christmas day bomber, and most important of all is the continuous vetting of issued visas. Like I mentioned in my remarks, at any time, the watch listing

system can be updated with new derogatory information from whatever source, and that will be vetted against the databases of issued visas, so if there is any match to a possible visa holder, we will review that and revoke it.

Mrs. MILLER. Thank you very much. I appreciate that information, and am very comforted to hear of those corrections being made. My final question I would ask of Mr. ICE—excuse me, Mr. Edge from ICE. You mentioned about the visa security units being in 19 countries, et cetera, and I know you talked a little bit about how that is happening in some of the high-risk embassies and the consulates, et cetera.

I thought it was interesting listening to Mr. Ramotowski talk about the Department of State and how you handle your agents in regards to language skills and various kinds of things. I am just wondering how you do with having your agents with language skills in these various areas. Also because, again, we are talking about budgetary considerations, I am not sure, but I would guess that it is very, very expensive to set up, to stand up such a unit in any of the consulates or embassies, and is there any way of replicating, maybe not 100 percent, but doing—I am not sure how many others you would like to have in a perfect world, what your optimal number actually is, is there any way of replicating that State-side to assist you from a budgetary standpoint, but really helping us prioritize again from a National security perspective?

Mr. EDGE. Well, certainly, the agency could always do more with more, but the Congress has been very, very helpful to us in setting up the current visa security programs in the various countries that we have them in.

Also hearing my counterparts' statements a little while ago from the consular perspective of the interviews that take place. During those interviews and the high-risk posts around the world, we would certainly have an ICE agent, special agent who is highly trained in investigations and interview techniques to sit with our Department of State counterpart. It would be a joint effort to determine whether or not admissibility should be granted and a visa should be issued.

As far as the expansion of the program, it costs about \$2.2 million to open up an office and \$2.2 million to continue the full operation of such a post. So we are doing the best we can, and we would welcome the continued support of the Congress in meeting the requirements of our mission. But our attempt to push the borders out and do a lot of this work overseas, as well as a lot of the vetting that we spoke about earlier on the domestic side, will certainly bolster our borders in countless ways.

Mrs. MILLER. Thank you.

Perhaps GAO could take a look at how that might happen State-side as well to do some of those kinds of things, not to tell you your business.

Mr. STANA. Actually, we have. We have looked at some of the efforts they have to not only do their work overseas but try domestically to do some of the screening via computer matches. There was one item, which I think was dropped from the budget before it went to OMB, I think it was a \$17 million line item, which would have enabled a match—matching law enforcement databases to

visa applications, which would have done the initial screening worldwide, \$17 million. Given the numbers he was talking about, it seems like it might be a bargain. We haven't looked at it to see if it was a bargain, but the numbers were right.

Mrs. MILLER. Very good. I appreciate you outlining that. I am sure my staff has taken a note of that. We are going to look at that as we proceed through our budgetary process here in the future.

At this time, the Chairwoman would now recognize Mr. Cuellar, our Ranking Member, for his questions.

Mr. CUELLAR. Thank you.

Before I ask my question, just to be fair to this current administration, everything depends on resources. I think what President Bush saw, what President Clinton and Bush No. 1 also saw the same thing; you can do as much as what Members of Congress give you, isn't that correct?

Mr. EDGE. That is correct, Congressman.

Mr. CUELLAR. Isn't it true also that the current administration has deported more criminal aliens than any other administration?

Mr. EDGE. That is correct, sir.

Mr. CUELLAR. By a lot larger number, is that correct?

Mr. EDGE. That is correct.

Mr. CUELLAR. All right. Thank you.

Let me go back to the original question I had, but before I ask you this thing about the flight training school in south Texas. Mr. Stana, I appreciate everything GAO. I am a big fan of what you all do. In your testimony, Mr. Stana, you stated that the 2010 airlines complied with the requirements that verify ESTA approval for almost 98 percent of the Visa Waiver Program's passengers prior to boarding. However, the remaining 2 percent, about 364,000 travelers travel without this Visa Waiver Program—without ESTA approval. Tell me what happened here in your opinion.

Mr. STANA. What seems to have happened in those cases—first off, the statistic went up to 99 percent. I think when we looked at that program, the 98 percent figure was from slightly prior, so it is getting better all the time.

In that case, I think it was a computer glitch where the computer was down, they couldn't get the ESTA verifications in on time. I have no idea how many of these ESTA inquiries result in a "do not board" or a stop for people. I don't think that data is tracked. I might be mistaken, but I don't think that data is tracked. But what we did see is that there were about 650 out of the number you cited that caused enough concern that, upon reflection, they said that they shouldn't have been allowed to board. But the computer was down; they couldn't get the assurances before the person boarded the plane.

Also, I should note that there is a timing issue here. You could submit the ESTA paperwork up to 2 years before a flight, and something could happen to you within those 2 years, you get a drunk driving conviction or something, which would result in an inability to board. All this really means is you have got to go to the consulate to get a visa manually as if this were not a visa waiver country.

Mr. CUELLAR. Gentlemen, for the other questions dealing with the south Texas—

Mr. WINKOWSKI. If I could just add just a little clarity there. When we started up with the ESTA system, we relied on the carriers to program this system so they could get a “no board” message. That took a little while, No. 1. No. 2, all ESTA applications are vetted on a continuing basis, like the visa. So if you have an individual that has applied for an ESTA, the ESTA is good for 2 years, and something happens in between that time that individual then is denied the ESTA and is notified to go to the embassy for a visa.

Mr. CUELLAR. Thank you.

Talk to me about south Texas. How do foreigners coming to the United States go to a flying school, training school on a tourist visa instead of a visa, and then how do we get agencies who start pointing the finger to each other and we can't seem to coordinate? Apparently, there were no terrorist ties to these students, at least from what I have been told, but it is just a little concerning that some other country can come in and do—you know, somebody from another country could come in and do the same thing and get some flight training. Whoever wants to handle this.

Mr. EDGE. In this particular instance, Ranking Member Cuellar, certainly the SEVP program didn't provide us with the information because the flight school was not registered with the program. You know, Praat was not a certified school at the time in September. What we have to do a better job of certainly is to communicate with our fellow Federal agencies, in this case the FAA, when they recognize that there are in fact people who are here on visitors' visas, a B-1 or B-2, who are enrolled in flight school when that should certainly be a F visa, N visa or a J visa, which would be more appropriate for that type of training.

If that were the case, we certainly would have had a little more vetting, and we would have been able to take a closer look at things. What we are doing now is taking a look at the flight school itself and conducting an investigation, the particulars of which I would be more than happy to offer you a briefing on outside of the scope of this hearing to give you a complete in-depth update, but there is certainly work to be done.

Mr. CUELLAR. Thank you.

I appreciate it. I appreciate a briefing at a later time on that. I would ask you to do that.

Gentlemen, my time is up. I want to thank all of you. I know that from the GAO, and I hope they listen to your good recommendations, and hopefully that you will take that in a constructive way what the GAO has given you. To all of you I really appreciate what you all do to keep our country safe. Thank you.

Thank you, Madam Chairwoman.

Mrs. MILLER. Thank the gentleman.

The Chairwoman now recognizes the gentleman from Florida.

Mr. BILIRAKIS. Thank you, Madam Chairwoman. I appreciate it very much.

For the panel or whoever would like to respond, what percentage of visa applicants are interviewed personally?

Mr. RAMOTOWSKI. Congressman, I will have to take that question back. It varies by country, and there is no set percentage that we apply. Most first-time applicants in most countries are interviewed.

Renewal applicants under certain circumstances can qualify for a waiver of that interview if they are renewing their visa in the same category within 12 months of the prior visa's expiration. So it would vary by country and by post.

Mr. BILIRAKIS. If you could get that information to me, I would really appreciate it very much.

Mr. RAMOTOWSKI. Yes, sir.

Mr. BILIRAKIS. Okay. With regard to the question that the Chairwoman asked with regard to the visa security units, I understand there are about 50 high-risk units identified by DHS, and it is ICE and the Department of State, and there are 19 in place. Can you please provide this committee with a progress report regarding the updated MOU between DHS and State?

Mr. EDGE. Certainly, sir, we would be able to provide that in writing at your request. We do have 57 high-risk issuing posts, and 19 are fully operational at this point in time.

Mr. BILIRAKIS. Okay. If you could get that to me, I would really appreciate it. Thank you.

I yield back, Madam Chairwoman.

Mrs. MILLER. Thank the gentleman.

The Chairwoman now recognizes the gentleman from South Carolina.

Mr. DUNCAN. Thank you, Madam Chairwoman.

First off, let me say, I am Scotch-Irish, and I used Ireland earlier in an example only. I don't want the folks in Ireland to say I was targeting their country. That happened one time when I mentioned the Northern border, and the Canadian press wrote something that I was talking of—it gets misconstrued. So no ire intended to Ireland at all.

Gentlemen, let me say first also that my ire is not directed at you or the agencies, but rather, I reflect the very passionate frustration of many, many Americans when it comes to immigration issues. It is in particular something that should be easier for us. From the folks in South Carolina looking at what Government does, they say this issue, visa-related immigration, should be easy because we are allowing guests to come into our country. We are giving them access through the visa process. It is not like they are just walking across our Southern border coming here, and that is a whole other issue of immigration, but we are issuing a visa. So it should be easier to make sure they don't overstay because we are giving them the ability to come here. I know I am simplifying matters in a lot of ways.

Mr. Winkowski, you have been sitting down there very patiently. I don't have a question for you, but I want to say thank you to you also. I met Chief Fisher a number of times, and I appreciate what you guys do.

My staff would like me to ask you a question, but I am really interested in the fact that if we have got Visa Security Program, if it is designated to be risk-based and the program is supposed to be active in the riskiest of countries, why are 11 of the top 20 high-risk posts not included? At high-risk posts where there are no visa security agents, what is the consular process for ensuring terror threats do not receive a visa?

I guess I will direct that to Mr. Edge.



Mr. EDGE. Well, the process to determine what posts are high-risk certainly is determined by the funding that is available. We also work very closely with the Department of State to determine at what posts would warrant based on the visa applications and other metrics, what posts would warrant a visa security unit overseas.

Mr. RAMOTOWSKI. Let me follow up, Congressman, if I could, from the State Department's perspective. We screen all our applicants as if they are high-risk in the sense that you can't guarantee where the next threat will come from. So all of our posts and all of our officers are trained to use our systems, to conduct intensive interviews and to be prepared to refuse visas to individuals who seek to do us harm, regardless of where in the world they actually apply for a visa. In this era of globalization, you can't predict where the next case will come from.

Mr. DUNCAN. Mr. Stana, what checks are not done with that regard?

Mr. STANA. You mean if the VSU is not at a post?

Mr. DUNCAN. Yes, sir.

Mr. STANA. It is just like Mr. Ramotowski said, they do a certain amount of vetting. The added security from the ICE person being there comes from their ability to use their law enforcement experience to maybe query another data set that isn't normally queried or ask the kinds of questions that a law enforcement background should give you.

But I would like to make one other point, Mr. Duncan. I think your point is a good one with the 11 of 20 high-risk posts not being staffed by VSUs. On the other end, there is a large number of the bottom 25 percent posts that are staffed with VSUs. I mean, there might be a rational reason why they would be there, but it would be good to reexamine that in the light that maybe some of those folks in the bottom 25 percent risk category, at least some of them, might be better served being in the top-risk posts.

Mr. DUNCAN. I know overseas service is very expensive, and so we have got CBP folks at overseas locations and consular affairs. Is there a way or are you looking at maybe bringing some of those people home that are stationed there and working more closely with U.S.-based? It is a flat world. We have got X-rays being looked at, they are taken here, looked at overnight in another country; it is a 24-hour cycle. So are we considering some of that to make it more cost-efficient? I will ask Mr. Winkowski that.

Mr. WINKOWSKI. Congressman, that is a very good question. What we have done in Customs and Border Protection is we have taken a hard look at our immigration advisory program that we have in eight countries of about 40 officers. We continue to evaluate the need to have officers in certain locations as well as the need to have them in different locations. So, for example, in Korea, we had made the decision that we did not need to have individuals at the airport in Korea, rather we could handle virtually, your point of the world being flat, that we could handle it out of our regional carrier liaison group out of Honolulu. So what happens is as that advanced information and that pre-departure information is sent through the system, that particular unit looks at that, identifies individuals that we believe are high-risk, perhaps has a visa that has

been revoked, perhaps is a TSDB, perhaps has some type of admissibility issue, and we coordinate with the host government and the airlines to prevent that person from going on the aircraft.

Conversely, there are other locations, for example Heathrow, very active, a lot of feeder flights in from areas of strategic importance, and we see a need to have those people there. So we are continuing to evaluate on a regular occurring basis, because as you point out, it is very, very expensive.

Mr. DUNCAN. So you have got a good relationship with the host countries is what you are saying?

Mr. WINKOWSKI. Yes, we do. We have a very, very good relationship.

Mr. DUNCAN. Madam Chairwoman, is there a way we can get the GAO to make sure, or request and to make sure that the ultimate—the most technology is being used to keep the costs down, but at the end of the day, we don't want any undie bomber to get on a plane and come to this country and create harm. So I appreciate what they do, but I also want to make sure we are getting the most bang for the buck for the taxpayer.

Mrs. MILLER. Absolutely. We will talk to the GAO about that and perhaps incorporate some of those requests in this letter that we will be drafting very shortly.

I thank the gentleman.

I thank certainly all of the panelists. I think this has been an excellent hearing. As we started at the outset talking about here we are on the 10th anniversary of the horrific, horrific attacks of our Nation on 9/11 and whether or not terrorists continue to exploit our visa system. It is clear from the testimony that we have had today that we have come a very long way, and I think we are making enormous progress and, again, as Mr. Cohen has outlined today a huge step forward.

But you know the largest room is always a room for improvement, and we have to continue to do that. Again, it is Congress' responsibility to provide the oversight to the various agencies, and it is our responsibility as well to budget the dollars and to make sure that the agencies understand our priorities and that we all work together cooperatively. I think we need to obviously continue to highlight some of our progress, but also not be afraid to take a very candid focus on what we need to do as a Nation to continue to secure our borders, to, as I mentioned at the outset, under our Constitution, our Constitutional responsibilities to secure our borders and to keep our citizens safe.

So I would also mention to the Members that if they have any additional questions, the hearing record will be held open for 10 days, and they can submit those questions for the record. Again, we thank all of our witnesses for coming today. The committee is adjourned.

[Whereupon, at 12:00 p.m., the subcommittee was adjourned.]