

**VISA SECURITY AND PASSENGER PRE-SCREENING
EFFORTS IN THE WAKE OF FLIGHT 253**

HEARING

BEFORE THE

**SUBCOMMITTEE ON BORDER,
MARITIME, AND GLOBAL
COUNTERTERRORISM**

OF THE

**COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES**

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

MARCH 11, 2010

Serial No. 111-55

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

58-301 PDF

WASHINGTON : 2011

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

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of
Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
WILLIAM L. OWENS, New York
BILL PASCRELL, JR., New Jersey
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
JAMES A. HIMES, Connecticut
MARY JO KILROY, Ohio
DINA TITUS, Nevada
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
PETE OLSON, Texas
ANH "JOSEPH" CAO, Louisiana
STEVE AUSTRIA, Ohio

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL
COUNTERTERRORISM

HENRY CUELLAR, Texas, *Chairwoman*

LORETTA SANCHEZ, California
JANE HARMAN, California
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
ANN KIRKPATRICK, Arizona
BILL PASCRELL, JR., New Jersey
AL GREEN, Texas
VACANCY
BENNIE G. THOMPSON, Mississippi (*Ex Officio*)

MARK E. SOUDER, Indiana
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan
PETER T. KING, New York (*Ex Officio*)

ALISON NORTHROP, *Staff Director*
NIKKI HADDER, *Clerk*
MANDY BOWERS, *Minority Subcommittee Lead*

CONTENTS

	Page
STATEMENTS	
The Honorable Henry Cuellar, a Representative in Congress from the State of Texas, and Chairwoman, Subcommittee on Border, Maritime, and Global Counterterrorism	1
The Honorable Mark E. Souder, a Representative in Congress from the State of Indiana, and Ranking Member, Subcommittee on Border, Maritime, and Global Counterterrorism: Prepared Statement	5
The Honorable Bennie G. Thompson, a Representative in Congress from the State of Mississippi, and Chairman, Committee on Homeland Security: Oral Statement	3
Prepared Statement	3
WITNESSES	
Mr. Raymond R. Parmer, Jr., Director, Office of International Affairs, U.S. Immigration and Customs Enforcement, Department of Homeland Security: Oral Statement	6
Prepared Statement	9
Mr. Thomas S. Winkowski, Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection, Department of Homeland Security: Oral Statement	12
Prepared Statement	13
Mr. David T. Donahue, Deputy Assistant Secretary for Visa Services, Bureau of Consular Affairs, U.S. Department of State: Oral Statement	17
Prepared Statement	19

VISA SECURITY AND PASSENGER PRE-SCREENING EFFORTS IN THE WAKE OF FLIGHT 253

Thursday, March 11, 2010

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

The subcommittee met, pursuant to call, at 11:32 a.m., in Room 311, Cannon House Office Building, Hon. Henry Cuellar [Chairman of the subcommittee] presiding.

Present: Representatives Cuellar, Thompson, Pascrell, and Souder.

Mr. CUELLAR [presiding]. The subcommittee will come to order. The Subcommittee on Border, Maritime, and Global Terrorism—Counterterrorism is meeting today to receive testimony on visa security, passenger pre-screening efforts in the wake of Flight 253.

Today the subcommittee is meeting to examine the visa security and passenger pre-screening efforts in the wake of the Flight 253 incidence—you know, happened around Christmas day of last year.

It is my hope that we build—we will be using this hearing to build on the hearing that the Chairman of the full committee had in January. We will be taking his foundation and work from there.

Mr. Chairman, we want to thank you, of course, for that.

Now that we have an understanding of the failures that left us vulnerable to attack, the subcommittee is examining as to what steps DHS, the State Department and the Federal and international partners are taking to address those vulnerabilities.

Along with other Members of this committee I recently had the opportunity to view some of those efforts first-hand. Last week I visited—we visited the Customs Border Protection National Targeting Center and was briefed by immigration and customs enforcement about the Visa Security Program.

I am encouraged by much of what has happened since that and, of course, what we have learned. Security in our skies starts with what we do on the ground.

I am glad that CBP is doing more than just screening passengers prior to departure for the United States, even though they have a limited number of physical presence at a number of the airports. They are making the most of existing technology and utilizing relationships with regional carrier liaisons, which makes good sense.

We must not forget that our airports are also the border ports of entry. That is why ICE is deploying additional units under its Visa Security Program, or VSP, as it is known, to strategic, high-risk visa issuing posts around the world.

However, more remains to be done. We need to look how CBP can further improve its pre-screening process to target those who seek to do us harm, without unduly delaying the legitimate travel. That balance is so important between security and, of course, commerce.

We also must explore whether we are making the most of the ICE Visa Security Program, and if it should be deployed to additional high-risk embassies and consulates.

Furthermore, we should examine how the State Department and the Department of Homeland can improve their coordination and their cooperation. The coordination, the cooperation, and communication is what we call the Three C's.

I have always advocated that as Government agencies, we should share more information. The more we can do together, the better it is for the people that we serve, our customers, our taxpayers, the people of America.

I know that ICE Assistant Secretary John Morton has been visiting our embassies to conduct outreach and discuss the program.

However, I do have to say that I was troubled that the State Department's recent denial of the VSP application for a post in the Middle East. My understanding that there is a sign of commitment to the interagency cooperation post-Flight 253, and clearly we have a ways to go on this.

But I was pleased to hear that since that, the State Department has reversed its decision, and hopefully that will set the tone for the future, and the cooperation between ICE and Homeland and the State Department is so important for us as the committee.

Of course, ICE and CBP are only part of the equation. Many of the problems that contributed to the Christmas day incident were intelligence and information-sharing failures. As Secretary Napolitano has stated, DHS is largely a consumer of the watch list.

We need to make sure we get ICE and CBP, as our frontline officers and agents at the—at America's land, sea, and airports the information they need so they can do their job in a proper way. Pre-screening passengers is one of our last lines of defense in securing our skies.

Also, Mr. Chairman, as you know, I want to thank you. This is my first hearing as Chairman of this subcommittee, and I certainly want to say thank you very much for that opportunity, Mr. Chairman.

Of course I will look forward to working with my Ranking Member, Mr. Souder, who has been very interested and very cooperative as we work in a bipartisan way.

Certainly, we want to do everything we can to address the border and maritime security matters that come before this subcommittee.

My approach as Chairman is going to be very simple. We want to work together. It is not us versus you. We are all on the same team. You might be the Executive branch. We might be the Legislative branch. But we should work together. There will be no surprises.

We are hoping, Mr. Chairman, that we get no surprises from our agencies also. If there is a problem, we would like to know before we read about it in the newspaper, as it happened in the past. I think it is a very simple request that we are making.

I think if we do that, Mr. Chairman, I think we can have a dialogue that will be for the betterment of the folks that we serve.

So I want to thank the witnesses for joining us here and for the courageous work that you all do every day and for keeping us safe. We want to say thank you. I look forward to your testimony and continuing our dialogue about how we can work together to make our Nation more secure.

I know our Ranking Member is not here. I know there are—they have a big meeting. But certainly, I would like to recognize the Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I associate myself with your earlier statement.

Logistically, they have just called six votes. That is the bad news. The good news—those are the only votes for the day, so hopefully we can, Mr. Chairman, adjourn and come right back. We can beg the indulgence of our witnesses.

You have made your statement quite clear. Cooperation and coordination is absolutely important in this process. The public expects no less. The assumption is that the right hand really ought to know what the left hand is doing.

In the spirit of cooperation and coordination, Congress has put the necessary tools in place with the professional help to make that happen. The missteps in Jerusalem you just talked about is unfortunate. Hopefully it won't happen again.

We have been assured, I think, at the staff level that that has been corrected and hopefully the State Department will work a little closer with us in the future.

I will, in the interest of time, Mr. Chair, include my formal statement for the record, and I will yield back.

Mr. CUELLAR. Without objection. Thank you, Mr. Chairman.
[The statement of Mr. Thompson follows:]

PREPARED STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

MARCH 11, 2010

In January, the Committee on Homeland Security held a hearing to examine the circumstances surrounding the attempted bombing of Northwest Flight 253 on Christmas day.

From our examination of the chain of events leading up to the incident, it is clear there were several failures that allowed the alleged perpetrator to board the U.S.-bound flight.

I am pleased that today's hearing will build on what we have learned by focusing on what we are doing, both now and over the long term, to eliminate the security gaps revealed by Flight 253.

As I stated earlier this year, we will not eradicate all terrorist threats overnight nor with a single technology.

Instead, we must develop a layered security approach that pushes borders out and begins far in advance of a passenger boarding a U.S.-bound flight.

With respect to the Department of Homeland Security, that will require a number of initiatives, including enhancing ICE's Visa Security Program (or "VSP") and strengthening CBP's passenger pre-screening activities.

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.

Mandating the Visa Security Program was one of these efforts.

By deploying experienced ICE agents at overseas posts, the program attempts to identify potential threats before they reach our borders.

Despite the legislative mandate to deploy Visa Security Units to high-risk posts, VSP expansion has been slow.

The current process can be cumbersome, and there appears to be some resistance to expanding the program.

I was troubled by the State Department's denial last month of ICE's application for a new VSP unit at a very strategic post—even in the wake of Flight 253.

At the same time, it is DHS' responsibility to ensure that applications are submitted in a timely way and that it makes the most of the positions granted.

In short, improved coordination and cooperation between DHS and the State Department are essential to the success of the program.

With respect to passenger pre-screening efforts, CBP has recently strengthened some of their processes to ensure greater scrutiny of certain passengers prior to departure, rather than waiting until they arrive at U.S. airports.

I want to hear more about those enhancements and what else we can do without unduly delaying legitimate travelers.

Those who would do us harm do not stick to the status quo, and we cannot either.

In closing, I would like to congratulate Representative Cuellar on his chairmanship. I look forward to continued good work from this subcommittee under his leadership.

I thank the witnesses for being here today.

Mr. CUELLAR. I guess at this time what we are going to do is we are going to excuse ourselves so we can go vote.

How much time do we actually have? About 10 minutes. Well, why don't we at least get the preliminary work out of the way? Let me do the introductions, so when we come back we can go ahead and get started.

So, Mr. Chairman, if you would allow me, first—our first witness, so we can do the introductions—our first witness is Mr. Raymond Parmer, Jr., who is the director of ICE Office of International Affairs, the largest international component within the Department of Homeland Security.

He has served in a variety of key ICE management positions, including as the deputy director of ICE Office of Investigations—again, the largest investigative arm of DHS.

With over 20 years of law enforcement experience, Mr. Parmer has served as the special agent in supervisory—special agent in a number of U.S. Customs Services Office of Investigation field and headquarters offices.

Again, Mr. Parmer, thank you very much for being here with us.

Again, our second witness, Thomas Winkowski, was first appointed assistant commissioner for the Office of Field Operations at Customs and Border Protection in August 2007.

In that position he manages an operating budget approaching \$2.5 billion, directs the activities of 24,000 employees and oversees programs and operations of 20 major field offices, 326 ports of entry, 58 operational Container Security Initiative ports and 15 pre-clearance stations.

Mr. Winkowski, again, we want to thank you. We got that tour of the center last week, and we want to thank you for your hospitality and the information that you provided us last week.

Our third witness is Mr. David Donahue, who has been the deputy assistant secretary for visa services in September 2008.

Mr. Donahue, thank you very much for being here with us.

Prior to that, he was the director of the Office of Policy Coordination and Public Affairs in the Bureau of Consular Affairs. He was a minister counselor for the consular affairs in Mexico City from 2005 and 2007. I guess you served there with my friend Tony Garza from South Texas, also, Brownsville, Texas.

Previous to that, he served at posts in the Philippines, Pakistan, Singapore, Trinidad, and Washington, DC. Mr. Donahue joined the Foreign Service in 1983.

Again, I want to thank all of you all for being here. Without objection, the witnesses' full statements will be inserted in the record, and we will ask you to hold at ease for a while, and we will be back right after the votes. Thank you very much for being here.

Committee recess.

[Recess.]

Mr. CUELLAR. All right. The subcommittee will resume again.

I believe Mr. Souder has a statement, and you want—you just want to go ahead and submit that for the record? Okay. Without objection, the record will be—the statement will be part of the record.

[The statement of Mr. Souder follows:]

PREPARED STATEMENT OF HONORABLE MARK E. SOUDER

MARCH 11, 2010

Thank you, Mr. Chairman. I would first like to congratulate you on the new subcommittee chairmanship. I know that we have had some briefings prior to this but this is your first official hearing as the Border, Maritime, and Global Counterterrorism Chair. I look forward to working with you over the rest of the Congress to examine issues under the subcommittee's purview.

I am pleased that we are here to examine visa security and passenger prescreening efforts in the wake of Flight 253. I also want to thank our witnesses for appearing before our subcommittee today to discuss this very important topic.

I want to say at the outset that, in my view, the Department needs to more aggressively strengthen its capabilities to improve visa security, bolster passenger prescreening, and expand border security efforts overseas to prevent potential terrorists from boarding airplanes bound for the United States.

The events of this past Christmas day show that terrorists remain committed to exploiting weaknesses in our homeland security and carrying out horrendous acts of violence against American citizens in a very coordinated and methodical manner.

I am quite concerned that our visa security and passenger prescreening efforts are not nearly as comprehensive and robust as they need to be to prevent someone like Umar Farouk Abdulmutallab from slipping through cracks in our defenses.

Unfortunately, we need only look at the Department's budget request for terrorist travel programs related to visa security and passenger prescreening to see those cracks. The Department's fiscal year 2011 budget request fails to sufficiently fund key programs and initiatives that can help identify terrorists seeking to travel to the United States. It represents a missed opportunity to expand border security efforts overseas and move toward a more coordinated strategy for expanding our Nation's security perimeter.

For instance, funding for the Visa Security Program, which places ICE personnel in high-risk locations overseas to more carefully scrutinize visa applicants, will not allow for expansion of this critical terrorist detection program in needed areas. ICE has identified several dozen locations in which Visa Security Units should be located, but insufficient funding and diplomatic resistance from the State Department has slowed its expansion, so much so that it would take many years to put units where ICE has identified that they are needed.

The budget for CBP eliminates funding for advanced passenger screening and targeting to help determine whether passengers should be prevented from boarding flights prior to their departure for the United States. These programs help assess potential passenger risk and determine whether heightened scrutiny of those passengers is necessary. CBP has acknowledged that this reduction will have an operational impact, but insists that the funds used for these programs are needed for

other priorities. I understand that there is intention to continue to fund this mission from within the base CBP budget, while a good step raises transparency issues and begs the question of what else is being cut.

The budget also fails to provide additional funding for tracking foreign students in the United States and would eliminate funding for the US-VISIT air exit, which is a key program necessary to identify visa overstays. It is extremely disconcerting that DHS would present a budget to Congress without funding or a plan to address this vulnerability.

These programs, and other existing capabilities to detect and disrupt terrorist travel, should be guided by a strategic plan designed to maximize our ability to connect-the-dots given appropriate information and further enhance the layered security necessary to stop future attacks. Congress has given the Department the tools it needs to push our border perimeter far beyond our physical shore so that terrorists are not able to get into the country to commit their despicable acts like they did on 9/11.

I am greatly troubled then that nearly 8½ years after the September 11 attacks, the Department either plans to scale back or fails to aggressively move forward on initiatives and programs that can help prevent a repeat of such terrible events.

I hope that we are going to hear from today's witnesses about how visa security has been improved and passenger prescreening has and can be further strengthened in the aftermath of the attempted bombing of Flight 253. I certainly have my doubts based on the Department's budget request for these areas for the coming fiscal year.

Mr. Chairman, I know that you are as committed as I am to ensuring that we are doing everything within our power to expand our border security efforts overseas to protect American citizens and prevent terrorists from entering our country. I hope today's hearing will provide insights to help us do that.

Thank you, Mr. Chairman. I yield back the balance of my time.

Mr. CUELLAR. At this time, as you recall—and again, we apologize. As you know, we have had different votes. We just finished, I believe, for the day, so what we will do now is that we will go ahead and start off with the witnesses.

Mr. Parmer, as you know, we just introduced everybody right before we left, so we will start off with Mr. Parmer. I would ask you to summarize your statement for 5 minutes, and then we will go on with Tom, and then other folks here will go ahead and ask the questions.

So, Mr. Parmer.

STATEMENT OF RAYMOND R. PARMER, JR., DIRECTOR, OFFICE OF INTERNATIONAL AFFAIRS, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, DEPARTMENT OF HOMELAND SECURITY

Mr. PARMER. Chairman Cuellar, Ranking Member Souder, thank you on behalf of Secretary Napolitano and Assistant Secretary Morton for the opportunity to discuss the international efforts of ICE to protect National security and prevent terrorist attacks.

Today, I would like to discuss the Visa Security Program in the context of the 9/11 Commission's findings, which emphasized the importance of our immigration system more thoroughly vetting individuals entering our country and developing functional counter-terrorism measures.

Within the Department of Homeland Security, ICE's Visa Security Program is one of a number of programs designed to protect the homeland and identify individuals who present a risk before they can harm the United States.

The Visa Security Program places ICE special agents in a U.S. embassies to work collaboratively with Department of State consular officers and diplomatic security agents to secure the visa adjudication process.

Before describing the Visa Security Program, the plans for expansion and challenges of expanding, let me describe ICE's international efforts more generally.

As the second-largest Federal investigative agency, ICE has a significant international footprint. Through our Office of International Affairs, ICE has 63 offices in 44 countries that are staffed by over 300 personnel.

ICE personnel in these offices collaborate with foreign counterparts 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, as well as facilitate repatriation of individuals with final orders of removal.

ICE's Office of International Affairs is also responsible for administering and staffing the Visa Security Program. The visa adjudication process is often the first opportunity our Government has to assess whether a potential visitor or immigrant presents a threat to the United States.

The U.S. Government has long recognized the importance of this function to National security. DHS regards the visa process as an important part of the border security strategy, and the Visa Security Program is one of several programs focused on minimizing global risks.

The Visa Security Program relies on trained, experienced investigators to look at an applicant in greater depth and examine their social networks and business relationships with a goal of developing information previously unknown to the U.S. Government to assess whether individual applicants pose security threats to the United States.

To conduct a thorough investigation, an ICE agent assigned to a Visa Security Unit must have the ability to interview the applicant of concern and must be exposed to local information to understand whether the applicant's affiliations raise any particular flags.

Each individual security—Visa Security Unit, with input from the State Department, develops a targeting plan based on assessed conditions and threats. Depending on the nature of the concern that an applicant poses a threat, the ICE agent's investigation may be complex and in depth, and in some cases taking months to complete.

Of course, not every investigation lasts months. ICE agents assigned to the Visa Security Program are experienced law enforcement agents who have spent years developing interview, interrogation, and other skills while investigating crimes in the United States.

Visa Security Program efforts complement the consular officers' responsibility for interviewing the applicant, reviewing the application and supporting documentation, and conducting automated screening of criminal and terrorist databases, with proactive law enforcement vetting and investigation.

ICE now has Visa Security Units at 14 high-risk visa adjudication posts in 12 countries. At these 14 posts, in fiscal year 2009, ICE agents screened approximately 905,000 visa applicants and,

with their State Department colleagues, determined that about 302,000 required further review.

Following investigation, in collaboration with State Department, ICE recommended refusal of over 1,000 applicants. In every instance, State Department followed the Visa Security Unit recommendation and ultimately refused to issue the visa. Visa Security Program recommendations have also resulted in State Department visa revocations.

Under the direction of the Homeland Security Council, beginning in May 2008, ICE and the State Department collaborated on the development of the Visa Security Program site selection methodology. The process for selecting a particular site for a Visa Security Unit begins with a site evaluation, which involves a quantitative analysis of threats posed and site assessment visits.

The DHS formal nomination process follows, which involves an analysis of ICE's proposal by DHS. Then, the National Security Decision Directive—38 process, which is a mechanism that gives the chief of mission in a particular post control over the size, composition, and mandate of full-time staffing for the post, commences within the State Department. Only once the chief of mission has approved an NSDD—38 request can ICE begin deployment.

ICE continues to look for opportunities to establish new offices overseas to screen and vet additional visa applicants at high-risk visa-issuing posts.

Based on collaborative site selection methodology with the State Department, ICE has conducted additional classified threat assessments in preparation for joint ICE-State Department site visits to embassies and consulates abroad.

Assistant Secretary Morton and his counterpart at the State Department are engaged now in a process of determining a common strategic approach to the broader question of how to collectively secure the visa issuance process.

I would now like to briefly discuss the security advisory opinion process, which is administered by the State Department and supported by other Government agencies to provide consular officers advice and background information to adjudicate visa applications abroad in cases of security or foreign policy interest.

In May 2007, Congress mandated the creation of a Security Advisory Opinion Unit within the Visa Security Program. The Visa Security Program now supports the SAO process and the Security Advisory Opinion Unit's findings are incorporated into the overall SAO recommendation used by consular officers to adjudicate visa applications.

The Security Advisory Opinion currently has co-located personnel at the Human Smuggling and Trafficking Center and CBP's National Targeting Center for Passengers and also has personnel assigned to the National Counterterrorism Center.

The integration of the Security Advisory Opinion Unit into these centers allows for real-time dissemination of intelligence between the various stakeholders in the visa adjudication process.

Again, thank you for the opportunity to appear before you today and for the subcommittee's continued support of ICE and our law enforcement mission.

Assistant Secretary Morton and I, in partnership with State Department, CBP and other vital partners, will continue collaborating to ensure the security of the visa while maintaining a fair and efficient process for legitimate visitors and immigrants to enter the United States.

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

[The statement of Mr. Parmer follows:]

PREPARED STATEMENT OF RAYMOND R. PARMER, JR.

MARCH 11, 2010

INTRODUCTION

Chairman Cuellar, Ranking Member Souder, distinguished Members of the subcommittee: On behalf of Secretary Napolitano and Assistant Secretary Morton, thank you for the opportunity to discuss the international efforts of U.S. Immigration and Customs Enforcement (ICE) to protect National security and prevent terrorist attacks. Today, I plan to discuss the Visa Security Program (VSP) in the context of the 9/11 Commission's findings, which emphasized the importance of our immigration system more thoroughly vetting individuals entering our country and developing functional counterterrorism measures. Within the Department of Homeland Security (DHS), ICE's VSP is one of a number of programs designed to protect the homeland and identify individuals who present a risk before they can harm the United States. The VSP places a DHS law enforcement officer (i.e., an ICE special agent) in a U.S. embassy to work collaboratively with Department of State (DOS) consular officers and Diplomatic Security Agents to secure the visa adjudication process. Before describing the VSP, our budget, the plans for expansion, and challenges of expanding, let me describe ICE's international efforts more generally.

ICE's Presence Overseas

ICE, as the second-largest Federal investigative agency, has a significant international footprint. ICE, through our Office of International Affairs (OIA), has 63 offices in 44 countries, staffed by more than 300 personnel. ICE personnel in these offices collaborate with foreign counterparts 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, and human smuggling and trafficking, and facilitate repatriation of individuals with final orders of deportation. In fiscal year 2009, ICE opened offices in: Amman, Jordan; Brussels, Belgium; Cartagena, Colombia; Guayaquil, Ecuador; and Jakarta, Indonesia and continued to expand its coordination with U.S. military commands, specifically United States Southern Command (SOUTHCOM), United States African Command (AFRICOM), and United States European Command (EUCOM). In fiscal year 2010, to increase our overseas presence and advance the efforts to investigate crimes that reach beyond our borders, ICE is proposing to open offices in Afghanistan, Israel, Vietnam, and Yemen.

ICE's OIA is responsible for administering and staffing the VSP.

The Visa Security Program

During the creation of DHS, Congress gave DHS some oversight responsibilities for the visa process. Specifically, Section 428 of the Homeland Security Act (HSA) of 2002 authorized the Secretary of Homeland Security to: Administer and enforce the Immigration and Nationality Act (INA) and other laws relating to visas; refuse visas for individual applicants in accordance with law; assign DHS officers to diplomatic posts to perform visa security activities; initiate investigations of visa security-related matters; and provide advice and training to consular officers. In short, the HSA directed DHS to assist in the identification of National security threats to the visa security process.

The visa adjudication process is often the first opportunity our Government has to assess whether a potential visitor or immigrant presents a threat to the United States. The U.S. Government has long recognized the importance of this function to National security. DHS regards the visa process as an important part of the border security strategy, and VSP is one of several programs focused on minimizing global risks. The VSP relies on trained law enforcement agents to look at an applicant in greater depth and examine their social networks and business relationships

with a goal of developing information previously unknown to the U.S. Government to assess whether individual applicants pose security threats to the United States. ICE agents assigned to Visa Security Units (VSU) are professional law enforcement agents who focus on selected applicants and any connection the applicants may have to terrorism. In the context of the visa security process, they begin by reviewing documents submitted by applicants, and reviewing the results of automated checks (from the Consular Lookout and Support System (CLASS), and others). To conduct a thorough investigation, an ICE agent assigned to a VSU must have the ability to interview the applicant of concern and must be exposed to local information to understand whether the applicant's affiliations raise any particular flags. Each individual VSU, with input from DOS, develops a targeting plan, based on assessed conditions and threats. Depending on the nature of the concern that an applicant poses a threat, the ICE agent's investigation may be complex and in-depth, in some cases taking months to complete. Of course, not every investigation lasts months. ICE agents assigned to the VSP are experienced law enforcement agents who have spent years developing interview, interrogation, and other skills while investigating crimes in the United States.

DHS does not participate in all visa adjudication procedures; rather, DHS becomes a part of the process following initial screening of an applicant. As such, where VSUs are present, DOS consular officers and ICE agents must establish effective and productive partnerships in order to enhance the security of the visa process.

VSP efforts complement the consular officers' responsibility for interviewing the applicant, reviewing the application, and supporting documentation and conducting automated screening of criminal and terrorist databases, with proactive law enforcement vetting and investigation. In carrying out this mission, ICE special agents conduct targeted, in-depth law enforcement-focused reviews of individual visa applications and applicants prior to issuance, as well as recommend refusal or revocation of applications when warranted.

ICE now has VSUs at 14 high-risk visa adjudication posts in 12 countries. While I can not identify the specific posts in this forum, I will gladly brief the Members and staff of this subcommittee in a classified or law enforcement-sensitive setting at a later date. At these 14 posts, in fiscal year 2009, ICE agents screened 904,620 visa applicants and with their DOS colleagues determined that 301,700 required further review. Following investigation, in collaboration with their DOS colleagues, ICE recommended refusal of over 1,000 applicants. In every instance, DOS followed the VSU recommendation and ultimately refused to issue the visa. VSP recommendations have also resulted in DOS visa revocations.

Expansion of the Visa Security Program

Under the direction of the Homeland Security Council, beginning in May 2008, ICE and DOS collaborated on the development of the VSP Site Selection Methodology. In brief, the process for selecting a particular site for a VSU begins with an ICE site evaluation, which involves a quantitative analysis of threats posed and site assessment visits. The DHS formal nomination process follows, involving an analysis of ICE's proposals by DHS. Then, the National Security Decision Directive—38 (NSDD—38) process, a mechanism that gives the Chief of Mission in a particular post control over the size, composition, and mandate of full-time staffing for the post, commences within DOS. Only once the Chief of Mission has approved an NSDD—38 request can ICE begin deployment.

ICE continues to look for opportunities to establish offices overseas to screen and vet additional visa applicants at high-risk visa issuing posts beyond the 14 posts at which we are currently operating. The fiscal year 2010 budget designated \$7.3 million for VSP expansion. With this funding level, ICE estimates that it can deploy to four additional posts. ICE has been conducting site visits and facilitating the NSDD—38 process in an effort to determine whether it would be beneficial to expand VSP operations to additional high-risk visa adjudicating posts. Based on collaborative site selection methodology with DOS, ICE conducted additional classified threat assessments on four posts in preparation for joint VSP—DOS site visits to embassies/consulates abroad. The VSP program has continued to grow since its inception. While ICE is continuing to expand the program, further expansion is contingent on ICE's dedicating existing overseas funding to these efforts and approval of NSDD—38 requests at the posts in question.

ICE will continue moving forward to deploy new offices to the highest risk visa adjudicating posts worldwide as resources allow, and will continue to conduct joint site visits with DOS to create opportunities for deployment. Moreover, ICE recognizes that the VSP is but one relatively small component in the Nation's counterterrorism strategy. Assistant Secretary Morton and his counterparts at DOS are en-

gaged now in a process of 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

To put the VSP discussion in perspective, I offer two brief examples of the results of including ICE in the visa process. In September 2008, DOS raised concerns about visa applicants sponsored by an international non-governmental sports group. ICE investigated and determined that the majority of past applicants sponsored by the group remained in the United States beyond their period of admission and that the sport group's president had three previous visa denials, with one on National security grounds. ICE disseminated information about potential future applicants throughout DHS and to DOS visa-issuing posts. This equipped CBP inspectors stationed at airports and the border and DOS consular officers with detailed information about the sports group to prevent future use of the club as a mechanism to gain entry into the United States, and to prevent National security threats from exploiting the scheme to gain entry.

Second, in July 2009, again while examining visa applications, ICE agents identified an Iranian national who applied for a visitor's visa to come to the United States to attend an information technology (IT) conference on behalf of his employer. Although the Security Advisory Opinion (SAO) process did not reveal a basis to find the Iranian national ineligible, ICE's review revealed that the Iranian national's employer—on whose behalf he was attending the IT conference—is an Office of Foreign Assets Control (OFAC)-designated organization allegedly used by the government of Iran to transfer money to terrorist organizations, including Hezbollah, Hamas, the Popular Front for the Liberation of Palestine—General Command and Palestinian Islamic Jihad. The visa applicant himself stated that he planned to attend the IT conference to explore the purchase of technology for his employer. While attending the conference alone did not render the Iranian national inadmissible, the combination of attending on behalf of his employer (an OFAC-designated entity) and the stated purpose to “explore purchasing options” for IT equipment constituted reasonable grounds for denial of the visa. Therefore, ICE recommended that DOS deny the visa on National security grounds, in accordance with the INA, as his purpose for coming to the United States was to possibly procure IT equipment for a designated OFAC organization. DOS concurred with ICE's recommendation and denied the visa.

I offer these examples to illustrate in real terms the benefit of a strong working relationship with DOS, and how the partnership advances the goal of preventing those who may intend to harm the United States from using a visa to enter our Nation.

The Visa Security Program's Security Advisory Opinion Unit (SAOU)

The Security Advisory Opinion (SAO) process is the mechanism administered by DOS, supported by other Government agencies, to provide consular officers advice and background information to adjudicate visa applications abroad in cases of security or foreign policy interest. In May 2007, Congress mandated the creation of a Security Advisory Opinion Unit (SAOU) within the VSP. VSP now supports the SAO process and the SAOU's findings are incorporated into the overall SAO recommendation used by consular officers to adjudicate targeted visa applications of National security or foreign policy interest.

The SAOU is currently operating a pilot program that screens visa applicants and communicates any potential admissibility concerns to DOS. The SAOU currently has co-located personnel at the Human Smuggling and Trafficking Center (HSTC), the National Targeting Center-Passenger (NTC-P), both located in the National Capital Region, and also has personnel assigned to the National Counterterrorism Center (NCTC). The integration of the SAOU into these centers allows for real-time dissemination of intelligence between the various stakeholders in the visa adjudication process.

CONCLUSION

I would like to thank the subcommittee for the opportunity to testify today and for its continued support of ICE and our law enforcement mission. Assistant Secretary Morton and I, in partnership with the State Department and other vital partners, will continue collaborating to ensure the security of the visa while maintaining a fair and efficient process for legitimate visitors and immigrants to enter the United States.

I would be pleased to answer questions you may have at this time.

Mr. CUELLAR. Thank you, Mr. Parmer, for your testimony.

At this time I will recognize Mr. Winkowski for 5 minutes for your testimony.

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

Mr. WINKOWSKI. Thank you, Chairman Cuellar, Ranking Member Souder, and thank you for the opportunity to appear today to discuss the steps U.S. Customs and Border Protection takes to pre-screen travelers bound for the United States.

I appreciate the committee's leadership and your steadfast efforts to ensure security of the American people.

Also, Mr. Chairman, I would just like to thank you for taking the time from your busy schedule to visit us at the NTC a few weeks ago.

Today I want to describe the role that CBP currently performs in aviation security and the enhanced security measures implemented in the aftermath of the attempted Christmas day attack.

As part of our efforts to screen passengers bound for the United States, CBP is an end-user of the U.S. Government's consolidated terrorist watch list, which we use to help keep potential terrorists off flights bound for the United States and identify travelers that require additional screening.

The majority of travelers bound for the United States are required to either have a visa issued by the Department of State or are traveling under the Visa Waiver Program, an electronic travel authorization issued through the Electronic System for Travel Authorization, most commonly referred to now as ESTA.

ESTA enables CBP to conduct enhanced screening of VWP applicants in advance of travel to the United States in order to assess whether they could pose a risk to the Nation. When a traveler purchases a ticket for the—for travel to the United States, a passenger name record may be generated in the airlines reservation system.

A PNR may contain various data elements such as itinerary, co-travelers, changes to the reservation and payment information. CBP receives PNR data from the airline at various stages, beginning as early as 72 hours prior to departure and concluding at the scheduled departure time of the flight.

CBP uses the Automated Targeting System to evaluate the PNR data against targeting rules. It is important to note that PNR data received by airlines varies and may be incomplete, thus resulting—reflecting different information than the person's actual travel documentation.

On the day of departure, when an individual checks in for his 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.

APIS data is far more complete and considered more accurate than PNR data. DHS screens APIS information on international flights to and from the United States against the Terrorist Screening Database, TSDB, as well as against criminal history informa-

tion, records of lost or stolen passports and prior immigration or customs violations.

At nine airports in seven countries, CBP officers are stationed under the Immigration Advisory Program. Working with CBP's National Targeting Center, IAP officers are provided information on certain passengers who may constitute a security risk.

These officers can then make no-board recommendations to carriers and host governments but do not have the authority to arrest, detain, or prevent passengers from boarding planes.

While flights are en route to the United States, CBP continues to evaluate the APIS and PNR information submitted by the airlines. At this point, a further assessment of individuals' admissibility into the United States is conducted and a determination is made as to whether an individual requires additional screening prior to admission.

Upon arrival in the United States, travelers present themselves to a CBP officer for inspection. Based on the information gathered during the in-flight analysis as well as the on-site CBP officers' inspection, which includes examining travel documents, observing and interviewing the traveler, a determination is made as to whether the traveler should be referred for a secondary inspection or admitted to the United States.

Since Christmas day, CBP has undertaken a number of steps to enhance our current process. We have expanded the information referred to IAP officers. We also began additional pre-screening of passengers traveling from non-IAP locations.

Officers assigned to our Regional Carrier Liaison Group, of which we have three around the country working for—working with the NTC, makes recommendations to foreign carriers to deny boarding to individuals traveling to the United States who have been identified as being a National security risk, are ineligible for admission, or are traveling on fraudulent or fraudulently obtained documents.

Through intelligence-sharing agreements, CBP continues to work with our foreign government counterparts as well as CBP and ICE attachés in order to share information as necessary and appropriate.

While we address the circumstances behind the specific incident, we must also recognize the evolving threat posed by terrorists and take action to ensure that our defenses continue to evolve in order to defeat them.

We live in a world of ever-changing risk, and we must move as aggressively as possible both to find and fix security flaws and anticipate future vulnerabilities.

Chairman Cuellar, thank you very much for the opportunity to testify, and I look forward to answering your questions.

[The statement of Mr. Winkowski follows:]

PREPARED STATEMENT OF THOMAS S. WINKOWSKI

MARCH 11, 2010

Chairman Cuellar, Ranking Member Souder, and distinguished Members of the subcommittee. Thank you for the opportunity to appear today to discuss the steps U.S. Customs and Border Protection (CBP) takes to pre-screen travelers bound for the United States. I appreciate the committee's leadership, and your steadfast efforts to ensure the security of the American people.

The attempted attack on Northwest Flight 253 on December 25 was a powerful reminder that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. As Secretary Napolitano has testified at recent hearings regarding the attempted attack, this administration is determined to thwart terrorist plots and disrupt, dismantle, and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This is an effort that involves not just CBP, but components across the Department of Homeland Security and many other Federal agencies as well as State, local, Tribal, territorial, private sector, and international partners.

Today I want to describe the role that CBP currently performs in aviation security and the enhanced security measures implemented in the aftermath of the attempted Christmas day attack.

CBP'S ROLE IN MULTIPLE LAYERS OF DEFENSE

Since 9/11, the U.S. Government has employed multiple layers of defense across several departments and agencies to secure the aviation sector and ensure the safety of the traveling public. Different Federal agencies bear different responsibilities, while other countries and the private sector—especially the air carriers themselves—also have important roles to play.

CBP is responsible for securing our Nation's borders while facilitating the movement of legitimate travel and trade vital to our economy. Our purview spans more than 5,000 miles of border with Canada and 1,900 miles of border with Mexico. CBP is the largest uniformed, Federal law enforcement agency in the country, with over 20,000 Border Patrol Agents operating between the ports of entry and more than 20,000 CBP officers stationed at air, land, and sea ports Nation-wide. These forces are supplemented with more than 1,100 Air and Marine agents, and 2,300 agricultural specialists and other professionals. In fiscal year 2009 alone, CBP processed more than 360 million pedestrians and passengers, 109 million conveyances, apprehended over 556,000 illegal aliens between our ports of entry, encountered over 224,000 inadmissible aliens at the ports of entry, and seized more than 5.2 million pounds of illegal drugs. Every day, CBP processes over 1 million travelers seeking to enter the United States by land, air, or sea.

In order to counter the threat of terrorism and secure our borders, CBP relies on a balanced mix of professional law enforcement personnel, advanced technologies, and fully modernized facilities and infrastructure both at and between the ports of entry. We deploy a cadre of highly trained agents and officers who utilize state-of-the-art technologies to quickly detect, analyze, and respond to illegal breaches across the borders. These personnel rely upon a solid backbone of tactical infrastructure to facilitate their access to border areas while impeding illegal entry by persons or vehicles into the United States. CBP Officers utilize advanced targeting, screening, and inspection technologies to quickly identify persons or cargo that warrant additional scrutiny without unduly impeding the traveling public or commerce.

CBP and Intelligence

In 2007, CBP created the Office of Intelligence and Operations Coordination (OIOC), which serves as the situational awareness hub for CBP, providing timely, relevant information, and actionable intelligence to operators and decision-makers and improving coordination of CBP-wide operations. Through prioritization and mitigation of emerging threats, risks, and vulnerabilities, OIOC enables CBP to better function as an intelligence-driven operational organization. The OIOC serves as a single, central repository for agency-wide intelligence, while exploring new ways to analyze and fuse information.

As part of our efforts to screen passengers bound for the United States, CBP is a consumer of the U.S. Government's consolidated terrorist watch list, which we use to help keep potential terrorists off flights bound for the United States and to identify travelers that require additional screening. Specifically, DHS uses the Terrorist Screening Database (TSDB), managed by the Terrorist Screening Center, as well as other information provided through the intelligence community, to determine who may board flights, who requires further screening and investigation, who should not be admitted, or who should be referred to appropriate law enforcement personnel.

National Targeting Center-Passenger (NTC-P)

A key tool for DHS in analyzing, assessing, and making determinations based on the TSDB and other intelligence information, is the National Targeting Center (NTC). The NTC is a 24/7 operation, established to provide tactical targeting information aimed at interdicting terrorists, criminal actors, and prohibited items. Crucial to the operation of the NTC is CBP's Automated Targeting System (ATS), a primary platform used by DHS to match travelers and goods against screening infor-

mation and known patterns of illicit activity. Since its inception after 9/11, the NTC has evolved into two Centers: the National Targeting Center Passenger (NTC-P) and the National Targeting Center Cargo (NTC-C).

This year, Immigration and Customs Enforcement (ICE) began deploying Visa Security Program (VSP) personnel to the NTC-P to augment and expand current operations. Through the VSP, ICE stations agents at embassies and consulates to assist the State Department in identifying visa applicants who may present a security threat. The focus of the VSP and NTC-P are complementary: The VSP is focused on identifying terrorists and criminal suspects and preventing them from reaching the United States, while the NTC-P 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-P has helped increase communication and information sharing.

Safeguards for Visas and Travel

One of the first layers of defense in securing air travel involves safeguards to prevent dangerous people from obtaining visas, travel authorizations, and boarding passes. To apply for entry to the United States prior to boarding flights bound for the United States or arriving at a U.S. port of entry, most foreign nationals need visas—issued by a U.S. embassy or consulate—or, if eligible to travel under the Visa Waiver Program (VWP) country, travel authorizations issued through the Electronic System for Travel Authorization (ESTA).¹

Issuing visas is the responsibility of the Department of State (DOS), which screens all visa applicants biographic data against the TSDB for terrorism-related concerns and screens their biometric data (fingerprints and facial recognition) against other U.S. Government databases for security, criminal, and immigration violation concerns. For individuals traveling under the VWP, DHS operates ESTA, a web-based system through which individuals must apply for travel authorization prior to traveling to the United States. ESTA enables CBP to conduct enhanced screening 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, including possible links to terrorism. On January 20, 2010, CBP began its transition to enforce ESTA compliance for air carriers, requiring all foreign nationals to present a valid authorization to travel to the United States at the airport of departure.

Pre-departure Screening

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, which may include optional 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 officers utilize the Automated Targeting System—Passenger (ATS-P) to evaluate the PNR data against “targeting rules” that are based on law enforcement data, intelligence, and past case experience.

On the day of departure, when an individual checks-in for their 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). APIS data, which carriers are required to provide to DHS at least 30 minutes before a flight for all passengers and crew on-board, contains important identifying information that may not be included in PNR data, including verified identity and travel document information such as a traveler's date of birth, citizenship, and travel document number. Carriers are required to verify the APIS information against the travel document prior to transmitting it to CBP. DHS screens APIS information on international flights to or from the United States against the TSDB, as well as against criminal history information, records of lost or stolen passports, and prior immigration or customs violations and visa refusals. APIS is also connected to Interpol's lost and stolen passport database for routine queries on all inbound international travelers.

Another layer in the screening process is the Immigration Advisory Program (IAP), which stations CBP officers at nine airports in seven countries in coordination with the host foreign governments. CBP's National Targeting Center provides the IAP officers with non-U.S. Citizen and non-Legal Permanent Resident matches to

¹Exceptions would be citizens of countries under other visa waiver authority such as the Western Hemisphere Travel Initiative or the separate visa waiver program for Guam and the Commonwealth of the Northern Mariana Islands, or those granted individual waivers of the visa requirement under the immigration laws.

the TSDB, of which the No-Fly list is a subset. CBP also flags anyone whose U.S. visa has been revoked, whose Electronic System for Travel Authorization (ESTA) has been denied, who is using a foreign lost or stolen passport, or who is included on a Public Health Record provided by the Centers for Disease Control and Prevention. IAP officers can make “no board” recommendations to carriers and host governments regarding passengers bound for the United States who may constitute security risks, but do not have the authority to arrest, detain, or prevent passengers from boarding planes.

Screening While En-Route to the United States and Upon Arrival

While flights are en route to the United States, CBP continues to evaluate the APIS and PNR information submitted by the airlines. At this point, a further assessment of an individual’s admissibility into the United States is conducted, and a determination is made as to whether an individual requires additional screening prior to admission.

Upon arrival in the United States, travelers present themselves to a CBP officer for inspection. 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 referred for a secondary inspection or admitted to the United States.

ENHANCED SECURITY MEASURES IMPLEMENTED SINCE THE CHRISTMAS DAY ATTACK

Following the first reports of an attempted terrorist attack on Northwest Flight 253 on December 25, DHS immediately put in place additional security measures. Since then, CBP has undertaken a number of initiatives to enhance our security posture.

IAP Referrals

As explained above, CBP officers stationed abroad under the IAP receive referrals from the NTC–P based on matches against the TSDB. Following the attempted attack in December, the NTC–P, in coordination with the OIOC, has expanded the information referred to IAP’s to include all aliens that the State Department has identified as actually, or likely, having engaged in terrorist activity as well, as existed in that case. NTC–P and OIOC continue to work with the intelligence community to develop new rules to address the ever-changing threat, while implementing specific operations to address these threats.

Referrals for non-IAP Airports

On January 10, 2010, CBP also began pre-screening passengers traveling from non-IAP locations through the ATS–P framework. To accomplish this goal, the NTC–P works in coordination with officers assigned to the Regional Carrier Liaison Groups (RCLG). The RCLG are established in Honolulu, Miami, and New York and provide regional points of contact and coordination between international carriers, foreign immigration authorities, and other DHS entities. The RCLG respond to carrier inquiries concerning the validity of travel documents presented or admissibility of travelers. Additionally, CBP officers at the NTC–P work with the RCLG officers to make recommendations to foreign carriers that boarding be denied (off-loads) to individuals traveling to the United States who have been identified as being National security related threats, ineligible for admission or who are traveling on fraudulent or fraudulently obtained documents prior to boarding a flight to the United States. However, the final decision to board or not board remains with the carrier. This pre-departure initiative mirrors our IAP efforts for flights originating from airports that do not currently have an IAP presence.

Enhanced Operational Protocols

At home and abroad, CBP officers have been briefed on the current threat stream and continue to work with our international partners, air carriers, local police, border control, and counterterrorism authorities to recommend passengers traveling to and entering the United States for additional screening as needed. CBP has implemented enhanced operational protocols at 15 preclearance locations and all 300-plus ports of entry in the United States. At airports, CBP has enhanced reviews of all incoming advanced passenger manifests based on current threats and have increased pre- and post-primary operations. At U.S. ports of entry, Passenger Analysis Units (PAU), and Counter Terrorism Response (CTR) teams continue carrying out targeted enforcement inspections, and have increased reviews of cargo manifest systems/databases by our Advance Targeting Unit (ATU) teams, and vehicle trunk inspections and truck cab checks. At POEs, the CTR team will normally be formed from CBP Officers assigned to special teams, or who possess prior counter-terrorism,

antiterrorism, or intelligence-related training or experience. These officers are then provided additional training in order to target persons or cargo that may warrant additional scrutiny. PAU and ATU are specifically designed to target passengers or cargo that may require CTR examination before they arrive at the POE. At sea-ports, CBP has heightened screening with Non Intrusive Inspection (NII) equipment of all cargo from countries of interest, and increased cargo and port perimeter sweeps.

Through intelligence-sharing agreements, CBP continues to work with our counterparts in the United Kingdom, Canada, and Mexico, as well as CBP Attachés and representatives around the world, to share information as necessary and appropriate.

CONCLUSION

The attempted attack on Christmas day serves as a stark reminder that terrorists motivated by violent extremist beliefs are determined to attack the United States. President Obama and Secretary Napolitano have made clear that we will be unrelenting in using every element of our National power in our efforts around the world to disrupt, dismantle, and defeat al-Qaeda and other violent extremists.

While we address the circumstances behind this specific incident, we must also recognize the evolving threats posed by terrorists, and take action to ensure that our defenses continue to evolve in order to defeat them. We live in a world of ever-changing risks, and we must move as aggressively as possible both to find and fix security flaws and anticipate future vulnerabilities. CBP will continue to work with our colleagues in DHS and the intelligence community to address this ever-changing threat.

Chairman Cuellar, Ranking Member Souder, and Members of the committee, thank you for this opportunity to testify. I look forward to answering your questions.

Mr. CUELLAR. Thank you, Mr. Winkowski, for your time. Again, thank you for that visit to allow us to be there at the center. It was very informative.

At this time, our last witness is Mr. Donahue.

Mr. Donahue, if you can summarize your testimony in 5 minutes.

STATEMENT OF DAVID T. DONAHUE, DEPUTY ASSISTANT SECRETARY FOR VISA SERVICES, BUREAU OF CONSULAR AFFAIRS, U.S. DEPARTMENT OF STATE

Mr. DONAHUE. Chairman Cuellar, Ranking Member Souder and—I want to thank you for another opportunity to share with you how the State Department is making the visa process more secure, the revocation process more expeditious, and how we are enhancing interagency information sharing.

The failed terrorist attack on Flight 253 revealed systemic failures in the U.S. Government's efforts to protect the people of the United States. The Department of State has been vigorously reviewing visa issuance and revocation criteria and determining how technological and procedural improvements can strengthen border protection.

Our immediate response to the Detroit incident was to direct our overseas missions to include complete information about any previous and current U.S. visas in all Visa Viper cables. That is happening now.

We also provided guidance on conducting a wide perimeter fuzzy search of our visa records.

We reviewed our visa revocation procedures. The State Department uses its broad and flexible authority to revoke visa to protect our borders. Since 2001 we have revoked more than 57,000 visas for a variety of reasons, including over 2,800 for suspected links to terrorism.

We are using this revocation authority as we review our visa records against records in our CLASS lookout database, our Visa Viper reporting, TSA's No-Fly and Selectee lists, as well as other sources. We confirmed that most individuals in these databases hold no visas. Of those few who did, a great many were revoked prior to the current review. We also revoked a number of visas in consultation with our partners.

We recognize the gravity of the threat we face and are working intensely with our colleagues from other agencies and our embassies and consulates overseas with the goal that no person who is known to pose a threat to our security holds a valid visa.

We have visa offices present in virtually every country of the world, staffed by consular officers drawn from the Department's professional and mobile multilingual foreign service officer workforce, trained in analytic interview techniques.

Our officers know that they are the first line of defense in border security. Our global presence, foreign policy mission, and personnel structure give us singular advantages in executing the visa function throughout the world.

Our officers know that U.S. security is paramount. Each 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 in continuing education places strong emphasis on border security and training in counterterrorism, fraud prevention, name checking, and other techniques.

Visa applicants are screened against DHS and FBI name-based and biometric databases as well as the 27 million names in our own CLASS database. Visas cannot be issued without further review for any applicant in the Terrorist Screening Database.

Applicants are also screened against our large and ever-growing facial recognition database. Our Security Advisory Opinion mechanism provides officers with the necessary advice and background information to adjudicate the cases of visa applicants with possible terrorist ineligibilities.

We are not afraid to say no. In fact, we denied more than 2 million visas in fiscal year 2009.

We also want to encourage legitimate travel to the United States. Tourism creates jobs for Americans and encourages understanding and appreciation of our values.

Within the Department we have a dynamic partnership between the Bureau of Consular Affairs, the Bureau of Diplomatic Security, the Office of the Coordinator for Counterterrorism and the Bureau of Intelligence and Research that add valuable law enforcement, investigative, and intelligence components to our capabilities.

We have 145 officers devoted to fraud prevention and document security world-wide. Seventy-three consular sections overseas have diplomatic security—assistant regional security officer investigator positions devoted to maintaining the integrity of the visa and passport process.

We are deploying an electronic visa application form which will provide more information to adjudicating officers and our partner agencies and facilities—and facilitate our ability to detect terrorism and fraud.

We are working with our interagency partners on the development and pilot testing of a new intelligence-based SAO system that will make full use of the additional application data.

We give other agencies immediate access to 13 years of visa data containing 136 million immigrant and non-immigrant visa records, and they use this effectively. In February 2010 alone, more than 18,000 employees of the Department of Homeland Security, Department of Defense, FBI, and Commerce made just over 1 million queries on our records.

We embrace a layered approach to border security screening and are fully supportive of DHS Visa Security Program. We have a particularly close and productive partnership with our DHS colleagues here.

DHS US-VISIT receives all the information we collect from visa applicants, including fingerprint data or use of ports of entry to confirm the identity of travelers.

Visa Security Units of the Immigration and Customs Enforcement, ICE, currently operate 14 visa adjudicating posts in 12 countries.

Since January 2010 chiefs of mission have received requests from ICE to open four VSUs and to augment staff at two existing VSUs. Using their authority, chiefs of mission have approved all four of the new VSUs and one request for expansion has been approved. The other is under review.

In closing, the Department of State is at the forefront of interagency cooperation and data sharing to improve border security. We understand the critical importance of our work. We have talented personnel and necessary tools to maintain safe borders that welcome the vast majority of legitimate travelers.

I am pleased to take your questions.

[The statement of Mr. Donahue follows:]

PREPARED STATEMENT OF DAVID T. DONAHUE

MARCH 11, 2010

Chairman Cuellar, Ranking Member Souder, and distinguished Members of the subcommittee, thank you for the opportunity to address you today. As a result of the attempted terrorist attack on Flight 253, the President ordered corrective steps to address systemic failures in procedures we use to protect the people of the United States. Therefore, the Department of State now is working on reviewing visa issuance and revocation criteria and determining how technological and other enhancements can facilitate and strengthen visa-related business processes.

As I have briefed the Members of the full committee on January 13, 2010, and as Under Secretary for Management Kennedy testified before the Senate Judiciary Committee on January 27, 2010, our immediate attention is focused on remedying shortcomings identified following the attempted attack on Flight 253. Planning for the future, incorporating new technology, increasing data sharing, and enhancing operational cooperation with partner agencies all contribute to a dynamic and robust visa adjudication process. We constantly review our IT systems and our procedures to adapt and improve our processes to respond to changing times, security threats and to incorporate new tools available to us. We have a highly trained global team working daily to protect our borders and fulfill the overseas border security mission and other critical tasks ranging from crisis management to protection of American interests abroad. Within the Department, we have a dynamic partnership between the Bureau of Consular Affairs and the Bureau of Diplomatic Security that adds a valuable law enforcement and investigative component to our capabilities. We use these strengths to address the continuing and evolving security threats.

In the case of Umar Farouk Abdulmutallab, on the day following his father's November 19, 2009 visit to the Embassy, we sent a cable to the Washington intel-

ligence and law enforcement community through the Visas Viper system that “Information at post suggests [that Abdulmutallab] may be involved in Yemeni-based extremists.” At the same time, the Consular Section entered Abdulmutallab into the Consular Lookout and Support System database known as CLASS, against which all visa applications are screened. In sending the Visas Viper cable and checking State Department records to determine whether Abdulmutallab had a visa, Embassy officials misspelled his name, but entered it correctly into CLASS. As a result of the misspelling in the cable, information about previous visas issued to him and the fact that he held a valid U.S. visa at that time, was not included in the cable. The CLASS entry using the correct spelling resulted in a lookout that was shared automatically with the primary lookout system used by the Department of Homeland Security (DHS) and accessible to other partner agencies. DHS has noted that, as a result of that record, they planned to meet Abdulmutallab and question him upon arrival.

We took immediate action to improve the procedures and content requirements for Visas Viper cable reporting that will call attention to the visa application and issuance information that is already part of the data that we share with our National security partners. All officers have been instructed to include complete information about all previous and current U.S. visa(s) when a Visas Viper cable is sent. This instruction includes guidance on specific methods to comprehensively and intensively search the database of visa records by conducting a wide-parameter, “fuzzy search,” leveraging an existing search capability called “Person Finder,” when searching our comprehensive repository of visa records in the Consular Consolidated Database (CCD). Searches conducted in this manner will identify visa records despite variations in the spelling of names as well as in dates of birth, places of birth, and nationality information.

In addition to this change in standard procedures on searching visa records, we immediately began working to refine the capability of our current systems. 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 27 million records found in CLASS. This strong searching capability has been central to our procedures since automated lookout system checks were mandated following the 1993 World Trade Center bombing. We use our significant and evolving experience with search mechanisms for derogatory information to constantly improve the systems for checking our visa issuance records.

The Department of State has been 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 has evolved as post-9/11 reforms were instituted and is now performed by the Terrorist Screening Center (TSC). All records added to the Terrorist Screening Database are checked against the Department’s Consolidated Consular Database (CCD) to determine if there are matching visa records. Matches are sent electronically from the TSC to the Department of State to 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 us by our consular offices overseas, our domestic visa office, DHS/Customs and Border Protection’s (CBP) National Targeting Center (NTC), and other entities. Almost every day, we receive requests to review and, if warranted, revoke visas for potential travelers for whom new derogatory information has been discovered since the visa was issued. Our Operations Center is staffed 24 hours per day/7 days per week to address urgent requests, such as when the person is about to board a plane. I frequently use the State Department’s authority to prudentially revoke the visa and prevent boarding.

Since the Presidentially-ordered Security Review, there have been exigent changes in the thresholds for adding individuals to the Terrorist Screening Database, No-Fly, and Selectee lists. The number of revocations has increased substantially as a result. As soon as information is established to support a revocation, an entry showing the visa revocation is added electronically to the Department of State’s CLASS lookout system and shared in real time with the DHS lookout systems used for border screening.

The State Department has broad and flexible authority to revoke visas and we use that authority widely to protect our borders. Since 2001, we have revoked more than 57,000 visas for a variety of reasons, including over 2,800 for suspected links to terrorism.

We have been actively using this revocation authority as we perform internal reviews of our data against watch list information provided by partner agencies. For example, we are re-examining information in our CLASS database regarding individuals with potential connections to terrorist activity or support for such activity.

We are reviewing all previous Visas Viper submissions and cases that other agencies are bringing to our attention from the No-Fly and Selectee lists, as well as other sources. In these reviews, we identified cases for revocation and we also confirmed that substantial numbers of individuals in these classes hold no visas and of those few who did, a great many were revoked prior to the current review. We recognize the gravity of the threat we face and are working intensely with our colleagues from other agencies with the desired goal that when the U.S. Government obtains information, no person who may pose a threat to our security, holds a valid visa.

Because individuals change over time and people who once posed no threat to the United States can become threats, revocation is an important tool in our border security arsenal; we use our authority to immediately revoke a visa in circumstances where we believe there is an immediate threat. At the same time, we believe consultation with National security partners is critical. Expedient coordination with our National security partners is not to be underestimated. Unilateral and uncoordinated revocation could disrupt important investigations undertaken by one of our National security partners.

Finally, the Department is reviewing the procedures and criteria used in the field to revoke visas and will issue new instructions to our officers. Revocation recommendations will be added as an element of reporting through the Visas Viper channel. We are in the process of providing additional guidance to the field on use of the broad authority of visa officers to deny visas on security and other grounds. Instruction in appropriate use of this authority has already been a fundamental part of officer training for years.

Beyond revocations, the Department of State is at the forefront of interagency cooperation and data sharing to improve border security, and we have embarked on initiatives that will position us to meet future challenges while taking into consideration our partner agencies and their specific needs and requirements. We are implementing a new generation of visa processing systems that will further integrate information gathered from domestic and overseas activities. We are restructuring our information technology architecture to accommodate the unprecedented scale of information we collect and to keep us agile and adaptable in an age of intensive and growing requirements for data collection, processing, and sharing.

We are the first line of defense in border 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 impacts. 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. Remember, the vast majority of the more than 2 million visas denied last year were denied for reasons unrelated to terrorism. Let me reiterate, however, that the Department of State is fully committed to protecting our borders and has no higher priority than the safety of our fellow citizens and the legitimate foreign visitors who contribute so much to our economy and society.

The State Department has developed and implemented intensive screening processes requiring personal interviews, employing analytic interview techniques, incorporating multiple biometric checks, all built around a sophisticated global information technology network. We have visa offices present in virtually every country of the world, staffed by consular officers drawn from the Department's professional, and mobile multilingual Foreign Service Officer workforce. These officials are dedicated to a career of worldwide service, and they 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 contribute to 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.

Consular officers are trained to take all necessary steps to protect the United States and its citizens during the course of making a decision on a visa application. Each 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. Consular officers receive continuing education, including courses in analytic interviewing, fraud prevention, and advanced security name-checking.

Consular officers refused 2,181,986 nonimmigrant and immigrant visas in fiscal year 2009 out of 8,454,936 applications. We now are renewing guidance to our officers on their authority to refuse visas with specific reference to cases that raise security concerns. No visa is issued without it being run through security checks against our interagency law enforcement and intelligence partners' data. And we screen applicants' fingerprints against U.S. databases as well. The results of these checks by consular officers and any fraud indicators are brought to the attention of VSU officers wherever they are posted abroad.

In addition, the Department of State's Security Advisory Opinion (SAO) mechanism provides officers with the necessary advice and background information to adjudicate these cases of visa applicants with possible terrorism ineligibilities. Consular officers receive extensive training on the SAO process, including namechecking courses that assist in identifying applicants requiring 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, to suspect that an applicant may be inadmissible under the security provisions of the Immigration and Nationality Act, consular officers suspend processing and institute SAO procedures.

CLASS, our primary visa screening watch list, has grown more than 400 percent since 2001—largely the result of this improved exchange of data among State, law enforcement, and intelligence communities. Almost 70 percent of CLASS records come from other agencies. We have enhanced our automatic check of CLASS entries against the CCD as part of our on-going process of technology enhancements aimed at optimizing the use of our systems to detect and respond to derogatory information regarding visa applicants and visa bearers. We are accelerating distribution to posts of an upgraded version of the automated search algorithm that runs the names of new visa applicants against the CCD to check for any prior visa records. This enhanced capacity is available currently at 83 overseas posts, with the rest to follow soon.

We are deploying an enhanced and expanded electronic visa application form, which will provide more information to adjudicating officers and facilitate our ability to detect fraud. Officers have access to more data and tools than ever before, and we are evaluating cutting-edge technology to further improve our efficiencies and safeguard the visa process from exploitation. We are working with our interagency partners on the development and pilot-testing of a new, intelligence-based SAO system that will make full use of the additional application data.

The Department of State has a close and productive partnership with DHS, which has authority for visa policy under Section 428 of the Homeland Security Act. Over the past 7 years both agencies significantly increased resources, improved procedures, and upgraded systems devoted to supporting the visa function. DHS receives all of the information collected by the Department of State during the visa process. DHS's US-VISIT is often cited as a model in data-sharing because the information we share on applicants, including fingerprint data, is checked at ports of entry to confirm the identity of travelers. DHS has broad access to our entire CCD, containing 136 million records related to both immigrant and nonimmigrant visas and covering visa actions of the last 13 years. Special extracts of data are supplied to elements within DHS, including the Visa Security Units of Immigration and Customs Enforcement (ICE). These extracts have been tailored to the specific requirements of those units.

We are working closely with ICE Visa Security Units (VSUs) established abroad and with domestically-based operational units of DHS, such as CBP's National Targeting Center. VSUs currently operate at 14 visa adjudicating posts in 12 countries. Since January 19, 2010, we have received requests from DHS's component, Immigration and Customs Enforcement, to open four additional VSUs and to augment staff at two existing VSUs. The Chiefs of Mission have approved the four new VSUs and one request for expansion; the other request for expansion is under review.

We make all of our visa information available to other involved agencies, and we specifically designed our systems to facilitate comprehensive data sharing. We give other agencies immediate access to over 13 years of visa data, and they use this access extensively. In February 2010 alone, more than 18,000 employees of DHS, the Department of Defense (DOD), the Federal Bureau of Investigation (FBI), and the Department of Commerce made just over 1 million queries on visa records. We embrace a layered approach to security screening and are fully supportive of the DHS Visa Security Program.

Working in concert with DHS, we proactively expanded biometric screening programs and integrated this expansion into existing overseas facilities. In partnership

with DHS and the Federal Bureau of Investigation (FBI), we established the largest biometric screening process on the globe. We were a pioneer in the use of facial recognition techniques and remain a leader in operational use of this technology. In 2009, we expanded use of facial recognition from a selected segment of visa applications to all visa applications. We now are expanding our use of this technology beyond visa 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 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, we have 145 officers and 540 locally employed staff devoted specifically to fraud prevention and document security, including fraud prevention officers at overseas posts. We have a large Fraud Prevention Programs office in Washington, DC, that works very closely with the Bureau of Diplomatic Security, and we have fraud screening operations using sophisticated database checks at both the Kentucky Consular Center and the National Visa Center in Portsmouth, New Hampshire. Their role in flagging applications and applicants who lack credibility, who present fraudulent documents, or who give us false information adds a valuable dimension to our visa process.

The Bureau of Diplomatic Security adds an important law enforcement element to the Department's visa procedures. There are currently 75 Assistant Regional Security Officer Investigator (ARSOIs) positions approved for 73 consular sections overseas specifically devoted to maintaining the integrity of the process. This year, the Bureau of Diplomatic Security has approved 48 additional ARSOI 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 on border security, based upon broadly shared information, provides a solid foundation. At the same time we remain fully committed to correcting mistakes and remedying deficiencies that inhibit the full and timely sharing of information. We have and we will continue to automate processes to reduce the possibility of human error. We fully recognize that we were not perfect in our reporting in connection with the attempted terrorist attack on Flight 253. We are working and will continue to work not only to address that mistake but to continually enhance our border security screening capabilities and the contributions we make to the interagency effort.

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 exchange 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.

We are facing an evolving threat. 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. The people 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 of State has spent years developing the tools and personnel needed to properly execute the visa function overseas and remains fully committed to continuing to fulfill its essential role on the border security team.

Mr. CUELLAR. I want to thank you very much.

Again, I want to thank all the witnesses for being here with us.

I remind Members that we have 5 minutes of questions per witness—for the witnesses, should I say, and I will recognize myself for 5 minutes.

Since it is only you and I, Mr. Souder, we are going to probably stretch that a little bit and be a little bit more flexible.

But let me first—let me just start off with some procedure work first. Deadlines. The only thing is, as I mentioned, I would ask you all and your Congressional liaison folks that when we ask for testimony there are certain time tables. I understand you all were looking at each other's testimony and got a little delayed.

But I would ask you to just make sure that if you are going to be late, I would just ask, please, you know, talk to our committee. Just give us a little advance notice that it is going to be late, and would ask you to just do that just as a housecleaning procedure.

For the State Department, how would you rate your Department's ability to communicate with ICE?

Then, ICE, I will ask you the same thing.

I know that there was—a particular situation got denied, and then of course, now they got approved. But how would you rate your ability to work together, Mr. Donahue?

Mr. DONAHUE. Thank you for the question, Mr. Chairman. I can't imagine that there are two U.S. Government agencies that work more closely than the Department of Homeland Security and the Department of State, particularly in border issues.

We were just talking during the recess that if we put together the number of times that we have been together and that different people in my office have been with people in the other offices, both in ICE and the Department of Homeland Security, just in the last couple months it would probably be in the hundreds, if not more.

In addition, on the ICE VSU program, we have assigned senior officers to that program since the beginning who travel with the members of the ICE team in site review. We do the same on visa waiver expansion.

So we have a very close relationship, meeting many times during the week, usually.

Mr. CUELLAR. Okay.

Mr. Parmer.

Mr. PARMER. Thank you, Mr. Chairman. I would characterize it similarly as my colleague from State Department. I think when the Homeland Security Act of 2002 mandated the creation of the Visa Security Units, there was some skepticism, perhaps, at various levels in the State Department.

But in every location where—and I visited several of these locations—where we have the Visa Security Units, without exception, the naysayers have been overcome and feel that our programs are complementary and serve as force multipliers.

Mr. CUELLAR. Okay.

Now, let me ask you—using the example of the Flight 253, I—and I listened to the three witnesses give us the testimony—can you just give me a little checklist of what we did and what we are doing now that is different, improved?

If you can break down into different steps, using the example of 253, what we are doing now that is different, that has improved, so we can provide better security?

Let's start with the State Department, because remember, where the individual started off, and there were calls to the embassy—let's go step by step as to—and then any time, Mr. Parmer, you want to come in, or somebody wants to come in—this is something that we are doing differently, because I am—we got lucky.

You know, we will—you know, we say we got lucky. I am now interested in looking forward. What are we doing to provide better security?

Mr. DONAHUE. Thank you, Mr. Chairman. I think the first thing is that we have sent out to our posts—and we know that there was a problem with the spelling and the search engine that was used by the officer to check to see whether the traveler had prior visas.

We have sent out new information about a much more robust search engine and instructions on the importance of getting that information into the Visa Viper cable and other information that they should put in the Visa Viper cable, so that when that arrives at the interagency community people have a little—a lot more to go on to determine whether they need to do more investigation on that.

We are going out to our posts—we have already had a good response to this on the Visa Viper reporting, where posts are coming in, they are telling us a lot.

We start right away, as soon as we receive that Visa Viper cable, discussing that traveler with our partners, particularly with the TSC, the Terrorist Screening Center, to determine that we are—to deconflict any possible conflicts with people they are watching. Then we revoke very quickly.

I think those are the—probably the two most important things in—and the other part is we have been spending a lot of time with our interagency partners in ensuring that the watch lists are as effective as they can be.

Mr. CUELLAR. Okay. All right.

Mr. Parmer.

Mr. PARMER. Mr. Chairman—

Mr. CUELLAR. Again, just like Mr. Donahue, just give us the checklist as to what we are doing now differently.

Mr. PARMER. That is a difficult question to answer, because the Visa Security Units have always maintained a high level of scrutiny for the—working in concert with the—

Mr. CUELLAR. But let's use—

Mr. PARMER [continuing]. State Department.

Mr. CUELLAR [continuing]. Let's lose—I am sorry, let's use the 253 as an example.

Mr. PARMER. What we have done since then is re-prioritize, that we have a list of high-profile posts at which we would like to open Visa Security Units. We have re-prioritized that list in light of some of the intelligence that has come out of the Christmas day incident.

Assistant Secretary Morton and others are having high-level discussions with the State Department about things that we can do differently in the future toward not only the screening process but also a more rapid deployment for the Visa Security Units.

Mr. CUELLAR. Mr. Winkowski.

Mr. WINKOWSKI. Mr. Chairman, at CBP we have done several major issues that I think are very, very significant, and let me kind of take this in bites as you asked.

At our IAP locations, the nine IAP locations, prior to 12/25, our 29 officers out there were getting—from a terrorist-related standpoint were getting notification on their hot list that we showed you

down at the NTC. They were getting individuals from the no-fly and the terrorist screening database on the terrorist-related side.

Then on the admissibility-related side, the ESTA denials, the visa revocation, lost or stolen passports, and the public health notifications, so that was prior to the Christmas incident.

Since then, we have grown the hot list—continue, of course, to get the no-fly. But we have also included the selectees, those individuals that are selected for enhanced inspection as part of the TSA program.

I wanted to make sure that as those individuals went through the selectee process that is conducted by security overseas that our IAP officers know that we have an individual going on that flight that was a selectee, so we can focus in and ask perhaps additional questions.

The other thing that we did was the SO-7 report that we referred to—

Mr. CUELLAR. Right.

Mr. WINKOWSKI [continuing]. A few weeks ago. That particular report was only sent to the port of entry domestically. It was not sent to the IAP locations.

A decision had been made early on in the program back in 2004, 2005 when we stood up the Immigration Advisory Program that we were very concerned that we could overwhelm the small number of officers that we have over in those locations.

So we wanted to make sure they got—you know, that the hot issues from the standpoint of the no-flies and the TSDB hits and the public health alerts—and the decision was made not to give them those particular reports.

I have changed that. All IAP locations now get that report. In this particular case, it was sent from State Department. Of course, we continue to have the ESTA denials, the visa revocations, the loss or stolen passports, and the public health. So that is the IAP piece.

The other major change that we made was as I was looking at the gaps and as you—as we talked—opportunities like this, you look at gaps. You look at, you know: What went wrong, what do we need to do better, where else are we vulnerable?

We have in those non-IAP locations we don't have any offices there, so you have individuals that perhaps had a visa that was revoked, would still get on that airplane and fly domestically—fly to the United States, and we would deal with that admissibility issue in the States.

What we have done is we had a unit called the Regional Carrier Liaison Group that you referred to in your opening comments and that I have referred to here, located in Miami, New York, and in Honolulu. That unit was stood up a number of years ago to really reach out to the airlines and work with the airlines on individuals with fraudulent documentation.

Recently down in Miami we have that group well entrenched for a number of years, and what we did was we took what were concerned with the IAP locations and overlaid it over into the Regional Carrier Liaison Group, so what we have is virtually a virtual net over the entire world from a standpoint of the Regional Carrier Liaison Group.

So what happens is when these—when an individual hits against our PNR or our APIS, and they are not at an IAP location, what happens is the National Targeting Center gets it on their hot list, calls the applicable Regional Carrier Liaison Group, who then notifies the airline overseas and tells the airlines that we have an individual, give them the name, that their visa had been revoked or there is an issue with them, and that we are recommending a no board.

We have 100 percent cooperation from all of the airlines on that. We are very, very good partners with them. So as a result of 12/25, not only did we enhance what we were doing at the IAP locations, we took it a step further and addressed the non-IAP locations as well.

The other thing that we have done is the hot list. It became apparent to me that, you know, we put the hot list out, and we really haven't—we really were not out there challenging that hot list. Do we have everything on that list that those officers need? I have implemented that procedure.

The other thing that we have done is all of these individuals that are on the hot list, referred over on the hot list, whether it is the IAP locations or the non-IAP locations, we have a FAM that is assigned to the National Targeting Center, and they are given that information on every single flight of individuals that are on our hot list.

So there is awareness if a FAM is going to be boarding that particular aircraft so he or she knows who is on that aircraft from a standpoint of any type of security issues.

Mr. CUELLAR. Okay.

Mr. WINKOWSKI. That is what we have done.

Mr. CUELLAR. Mr. Winkowski, let me just—I don't want to complicate this, because we have been talking about airports, and some of those lists are for the airlines, but as you know, 88 percent of the goods and services come through land ports, roughly.

Are we doing any additional screening for our land ports? That is where—I mean, that is basically where most of our people will be coming in. I know some of those lists are—I understand that. But anything else extra that we are doing?

Mr. WINKOWSKI. Well, on the land border side, of course, we have implemented the Western Hemisphere Travel Initiative, with standardized documents, which as—you know, as you mentioned, you know, we have job and field operations of balancing preventing dangerous people and dangerous things from coming into the country, but at the same time expediting legitimate trade and travel.

So certainly, I think the Western Hemisphere Travel Initiative has helped us standardize documents, and what we are seeing over time here is we have a very, very high compliance rate down on the southwest border, for example. We are about 92 percent compliant.

We have moving much quicker towards getting the RFID readable documents that the individuals can have—for example, State Department is reissuing the border crossing cards. There is 10 million border crossing cards. They are coming up. They are expiring. The State Department is reissuing them with the RFID chip.

So you have got that piece. We have a targeting piece. We have an automated targeting system for land. It is a robust system, but you don't get that pre-departure information on the vehicle side, that we deal—we don't have advance information on who is coming into the United States on the land border side.

We have it on the cargo side, but we don't have it on the—on the people side, and I think that is something that we need to work towards, and I will make a suggestion on that in a moment.

So you know, we have got targeting units. Our query rates are much higher than they have ever been. Not so many years ago, because of infrastructure problems and because of a lack of the right technology, i.e. the WHTI solution, we had a relatively low query rate.

We have grown that tremendously. On the southwest border we are over 70 percent query rates, and our goal is to be at 100 by the end of this fiscal year. So we have that layered approach in there. WHTI has been extremely helpful to us and certainly appreciate what Congress has done to give us a steady stream of funding for WHTI.

But I do think it is time from a standpoint of looking at kind of an all modes APIS, advanced information all modes, because we do have ferries out there that don't have any advance information. Trains are voluntary. Buses—and—

Mr. CUELLAR. Right.

Mr. WINKOWSKI [continuing]. Certainly, I don't need to explain to you buses coming into Laredo. It is the busiest bus location. We need to work towards a solution of getting advance information for those bus travelers.

Mr. CUELLAR. Right, and I think working with Mr. Souder and Mr. Thompson and the other Members and our staff, that is an issue that we want to talk about at a later time, because, like you mentioned, there are other modes of transportation in the United States that have no advance notice.

Mr. WINKOWSKI. Right.

Mr. CUELLAR. If somebody gets smart out there, all they have to do is look at the other modes of transportation and again, keeping in mind, 88 percent of all the goods—people coming into the United States are coming through land ports, and I know the focus—because of Flight 253 and this is why we are here.

Let me just finish one thought, and I am—if the Ranking Member will indulge me on this, and then I will give him all the flexibility he needs to get.

So we talked about the protocols were in place for Flight 253. We talked about that you just gave me a little summary of the new protocols that you all added.

Using the new protocols, the new changes, using the individual from Flight 253 that happened last year, under the new protocols, where would you have picked up this individual?

Mr. WINKOWSKI. What would have happened with the new protocols—he would have hit against the SO-7 report, the State Department report, and the quasi visa refusal.

That report would have been—that record would have been placed on the hot list for the IAP in Amsterdam. What would have

happened is the IAP officer would have taken the individual and begun the process of questioning him.

Mr. CUELLAR. Right. Now, what I understand—he was only interviewed by CBP when he landed in Detroit.

Mr. WINKOWSKI. That is correct.

Mr. CUELLAR. How would this have changed under the new protocols?

Mr. WINKOWSKI. Well, it would have been placed on his hot list. Prior to 12/25, the SO-7 report was not put on the hot list. It was viewed as an admissibility issue that—which we could handle State-side, because there is a series of Q&As that you have to do with the individual and IAP is not designed for that.

What we have done is for those terrorist exclusion codes for the SO-7—they are on the—now the hot list, so that would have come up through either the PNR or the APIS.

Mr. CUELLAR. Right.

Mr. WINKOWSKI. Our officers in Amsterdam would have notified. We would have gotten the passenger and questioned him in Amsterdam.

Mr. CUELLAR. Okay, good.

Mr. Donahue and then Mr. Parmer, same question. Under your new protocols, new changes, using the example of the individual on Flight 253, where would you have stopped this individual from your perspective?

Mr. Parmer, same question.

Mr. DONAHUE. Thank you very much, Mr. Chairman. I think today two things would have happened. First of all, the officer in Nigeria would have known that the traveler had a visa because they would have been using a more robust search engine.

They would have reported that in the Visa Viper cable, and also we would have their entry in a—as a P3B with the entry that my colleague just referred to.

Both of those—we are doing constant review of our lists. Any time we get a Visa Viper in, we look at that case very seriously.

A case like this I think we would have—you know, it is hard to predict, but I think we would have decided to revoke the visa, ask him to come back in to interview, so he wouldn't have had a visa and wouldn't have—wouldn't have traveled at all.

Mr. CUELLAR. Okay. So you feel under the new protocols you would have—using that as an example, you would have stopped him before he boarded.

Mr. DONAHUE. For example, there are no—no one with this code, this P3B code—there is no one in our records with a P3B code right now who has a visa.

Mr. CUELLAR. Okay.

Mr. Parmer, same question. New protocols, how would this have been different for that individual?

Mr. PARMER. Chairman, it would purely be speculative on my part to—

Mr. CUELLAR. We understand. But under the new protocols—

Mr. PARMER. Well, there are no—from the perspective of the Visa Security Units, there are no different protocols. We were not in the post where the visa was issued, so it would be, again, purely speculative for me to comment on that.

Mr. CUELLAR. Okay, fair enough.

All right, Mr. Souder, thank you for your indulgence, and you have got 15 minutes of questioning.

Mr. SOUDER. Basically, it is the same thrust continued.

So, Mr. Parmer, are you in Nigeria now?

Mr. PARMER. No, sir.

Mr. SOUDER. Did you apply to go to Nigeria now? It is one of the more risky countries we have been seeing a lot in the news.

Mr. PARMER. Yes, sir, it is on the list of countries that we would like to establish a post in. I referenced earlier re-prioritization of the—of our high-risk list that we have worked on collaboratively with the State Department, and it is—

Mr. SOUDER. Is it a funding question?

Mr. PARMER [continuing]. Higher on the list. No, sir, it is not.

Mr. SOUDER. If it gets re-prioritized to go up, does one get bumped off where you had requested?

Mr. PARMER. Not of those currently pending, or the—of the NSDD-38s that were just approved, no, sir.

Mr. SOUDER. So you can add—there is no problem with adding countries? I am trying to figure out why it isn't there. You said that it—you are re-prioritizing to move it up higher.

Does that mean you didn't request it before, or it was below the funding cut for it before? I am trying to figure out what is the problem here. Is it a funding question?

Is it a staffing question, which when—then would probably be a funding question? Is it an embassy personnel? Is the State Department saying, "We can only absorb so many in a given year?"

Mr. PARMER. No, sir. No, sir. Before the Detroit incident, it was not ranked as highly on the list. We have been working under a 5-year expansion plan that was approved by the Homeland Security Council, and it is—with the infrastructure and the budget that we have in place, we have been seeking expansion that we were able to support.

So it hasn't been a funding issue or a State Department issue. It was just not as high on the list.

Mr. SOUDER. So Congress mandated that you go to 50, and how many are you now, 10, adding four?

Mr. PARMER. We are in 12 countries at 14 locations.

Mr. SOUDER. So since it is a mandate, why haven't you requested to move faster? I am trying to figure out what is the holdup.

Mr. PARMER. The best way to put that, again, is I will refer back to the expansion plan that was approved by the Homeland Security Council that—where we were moving forward at a rate that our infrastructure could support and as well as the budget—

Mr. SOUDER. By the infrastructure, you mean number of agents? Is this a computer question? It is not a computer question.

Mr. PARMER. No, sir.

Mr. SOUDER. It is not infrastructure that way. It is personnel?

Mr. PARMER. Our headquarters component, our administrative function, as well as the—what we could support through deployment of personnel.

It is too cumbersome to try to deploy that many people in a short period of time, and it was something that we could—our agency could comfortably—

Mr. SOUDER. Could you—

Mr. PARMER [continuing]. Move forward with and responsibly move forward with.

Mr. SOUDER. Could you get back to me with the particulars of what is so cumbersome about this? I am trying to—is it that you have to divert so many agents from other tasks to go there?

Is it that, quite frankly, it takes a long time to do the research, you don't have enough research personnel? I am trying to figure out what it is, because we said 50.

The irony here is—in this discussion is that I remember when I was over at the Government Reform Committee, and we first debated whether homeland security was going to go in there.

Initially, we were going to take the entire—and I worked with Chairman Ben Gilman at the time—take the entire security process away from the State Department. We worked out a compromise because you were supposed to be in all high-risk countries immediately after 9/11. This was a negotiated deal.

Because partly, visa clearance and that process is a key part of the State Department entry level training program. They had language background. When you actually got into it, it was better to work a cooperative process.

Now what I am finding—it has been a little while since 9/11, and we are in 2012, and you are resource-challenged, and I am just trying to figure out where it is. Did Congress turn it down? Did you not make a request? Are you being blocked from the request from OMB, which would be typical in many agencies? We understand that.

But the bottom line is that—and also I am a little perplexed why Nigeria wasn't there, but that is another question.

Now let me move to another aspect of the—kind of the same line of questioning. I was listening with interest as to what is changed, because that is one of the fundamentals, and first, if I could start with Mr. Donahue—well, let me ask Mr. Winkowski—good to see you.

One of the challenges here of anybody watching is that they think there is just like all these initials wandering around at every airport and port of entry. That was one of the most amazing performances of numbers of—it would have taken your testimony twice as long as if you would have spelled out all what those initials were of the different programs.

But in the challenge of—my understanding is CBP had the name right. It wasn't a spelling question for CBP and ICE, correct?

Mr. WINKOWSKI. That is correct, yes.

Mr. SOUDER. But you felt that the information wasn't actionable enough prior to getting on the plane, that it had to be done in Detroit.

Mr. WINKOWSKI. Yeah, a decision had been made when we stood up the IAPs back in 2004 that those kinds of reports, the quasi visa refusals—his visa was not canceled—could be handled State-side rather than at the IAP location, okay, because what we are concerned with is the program is very small, and we wanted the individuals assigned to the IAP locations to be focusing in what was on the hot list, and at that time these reports were not on there.

So Detroit got the report, and that was what was supposed to happen. The IAP location did not get that report.

Mr. SOUDER. Okay. Now, one of the confusing things for me, just trying to sort through—Mr. Donahue, you have suggested that probably, had you spelled it right and had this information, that now this person wouldn't be allowed a visa.

I am trying to figure out why would it be actionable for you to deny an interview and not for CBP, because they determined that information—is there a change in what is now actionable?

Mr. DONAHUE. Thank you for the question. There is. We certainly have looked at everything we do, and one thing that I think that we did before this incident was we sent in reports.

I don't know that all of us—I certainly didn't have as full an understanding of the entire interagency process for determining when a name gets promoted to watch listing.

We sent in the reports. We waited to see how that name would come out. Would it come out as a watch listing name? Would it be something that would go into a TIDE file and not be promoted?

We did not review all of the Visa Viper cables for a determination of revocation then, although the consular officer has the authority to make a recommendation to do an SAO, for instance.

So I think the real change here is that we—as soon as we get a Visa Viper cable in now, we are reviewing it ourselves also, and if there is information that makes us concerned that this person may have connections to terrorism, we are going to the interagency, we are saying we would think that we may be—want to revoke this visa, to have the person come in for an interview.

If there is no objection, we revoke.

Mr. SOUDER. One of the somewhat disturbing things that we heard—because one of the initial defenses was, “Well, we get family members and people coming in all the time who—who say things,” which is certainly true. There is all kinds of quarrels all over the world where people make cases.

But this person had been a fairly credible source before. Are you making those kind of—in our system, do we have some of those kind of cuts that we are becoming a little more aware of?

Mr. DONAHUE. Well, certainly, everyone is very sensitive to this type of reporting now. I also think that the information was very thin. It was that he had—as you know, the only information the consular officer had was that the son had come under the influence of extremists in Yemen.

That rings lots of bells today and certainly would, I think, any of us would revoke at that point.

Mr. SOUDER. I mean, did that not suggest something might be imminent?

Mr. DONAHUE. It is hard to say. It is hard to be in someone else's mind. But it could be that something is imminent or that the father would like us to use whatever assets we might have had in another country to find his son. Looking back, we could look at it that way.

But I think it is hard to reconstruct. I think today we certainly see—we have had a lot of threat reporting since then. I think that is another item that—to answer the Chairman's question, it is another item of things that we are doing—is that there is a much

more robust review of threat assessments and review of this kind of information against threat assessments.

Mr. SOUDER. Basically, meaning that when we get scared, we tilt towards caution and re-interviewing? I mean, that is kind of what it sounds like here, because—that we relax. I mean, it is not just any individual. I mean, the whole system seems to relax, including Congress—relaxes, and then we get scared, and then we tilt it.

It just seems to me we ought to have a pattern that when there is doubt you take extra caution.

Mr. DONAHUE. That is why we have put in—I think all of us have put in new systems. But for ourselves, we get a Visa Viper in, we will review that immediately, we will discuss it with the interagency and revoke. When we receive a request from NTC to revoke, we will review that case and revoke quickly. We understand the critical nature of this.

Mr. SOUDER. The January 27 hearing, I ask for the number of visa revocations per year and the number revoked based on terrorism concerns. Do you have that at this point, or what is the status of that request?

Mr. DONAHUE. Yes, it was in my statement. It was—

Mr. SOUDER. Okay. So you have it in the statement with the numbers?

Mr. DONAHUE. It is in the statement and in the—also the—yeah, the—

Mr. SOUDER. We may have some additional breakdown questions, and be interested—because I think it would be useful just for the Department and assuming that our regular oversight is going to see how that changes.

Now, obviously, if it changes over time, they are going to change their systems, too, so to a degree you are effective, you know, that doesn't—just because it goes up or down doesn't necessarily prove anything.

But initially, it will be interesting to see whether, in fact, more are revoked or less, or what the patterns are.

Mr. DONAHUE. You mean how many we have revoked since—

Mr. SOUDER. No, the original January 27 question and then, say, if you can continue to track that data—

Mr. DONAHUE. Okay.

Mr. SOUDER [continuing]. It is likely to—

Mr. DONAHUE. We will do that. We—

Mr. SOUDER [continuing]. Question.

Mr. DONAHUE [continuing]. The number is that we have revoked 57,000 since 2001 and 2,800 of those are terrorist-related. But we will continue to track that number. I think it is an important number, too.

Mr. SOUDER. Then for Mr. Wiskowski, that—you said—or Winkowski. I said “Wis,” sorry. Winkowski. In the last part you were—in response to his question, you talked about the—for example, the Staten Island and the Washington ferry systems and coming across from Canada where we caught the Millennium bomber—the trains and so on—that all challenges—any of those come through in a budget request to address it?

Mr. WINKOWSKI. No. What we are doing is we are beginning the process of studying how we ought to go about this. Now, for exam-

ple, buses—I think it is going to be very, very challenging, and we have got to find the right solution for us as well as the industry.

So I do not believe any requests came up for budget. We do have our WHTI office looking at these different modes and how we are going to accomplish that. We just recently, over the last year or so, put in eAPIS for general aviation, and it has worked out very, very well.

We have got very, very high compliance. But I think those four areas—and I didn't get to say small boats. I think the small boats also coming back and forth—getting some type of advance information with the technology that is out there today—we have done it with general aviation.

I think we have now got to lean forward here and really—again, to drill down on what would it take to get advance information on those modes.

Mr. SOUDER. A problem I have—because I believe that was a very sincere answer, but having worked narcotics prior to 9/11 and continuing to work the border questions, and having been in San Diego looking at the small boat question, looking at the aircraft question, north and south border, looking at Lake Champlain, we knew this was a problem before, like, the last 24 months.

Why are we just starting to develop the solutions now?

Mr. WINKOWSKI. Well, we have put in different boating—for example, small—

Mr. SOUDER. Yes.

Mr. WINKOWSKI [continuing]. Boats—and I think we both would agree it is a—it is a—

Mr. SOUDER. Incredibly challenging.

Mr. WINKOWSKI. Incredibly challenging, and—

Mr. SOUDER. The Great Lakes, with all the islands.

Mr. WINKOWSKI [continuing]. And we have got small boat strategies in there, and we have got the Air Marine working at—looking at northern border strategies from a standpoint of how to handle it with the Coast Guard and really, the Coast Guard is the lead on—in a lot of this area.

But you know, quite frankly, you know, we spend a lot of our time on containers, dealing with containerized cargo, whether it is the challenges we have there, with 100 percent scanning. A lot of intellectual capital goes into those program areas.

We are now beginning to really get—drill down on this area—ferries, and trains, and buses and small boats, and I—and there is also—there is a legislative fix.

As I understand it, sir, we need legislation in order to mandate that, or the legislation that you all gave us for the cruise ship industry and the airlines and the other modes that we have out there requires a legislative vehicle, as I understand it.

Mr. SOUDER. My concern with this—and I encourage you to do this. I encourage your agency to do this—is somebody has to be working in a non-panic mode. When people say what do you do for a living, I say I am a Congressman; we overreact for our business. That is our duty, because we are like the weathervanes of society. We run every 2 years, which means constantly we blow with that.

But somebody has got to be saying what is comprehensive. We just can't have, "Oh, we are really fortunate this guy didn't know

how to do his bomb.” We have to be anticipating. We have to have you leading.

It is like, “Oh, we are going to do 100 percent of cargo here,” without understanding kind of risk assessment—how are you doing on the south and north border, how are you doing on the ports, how are you doing on the containers.

Look, because as we learn in this case, they probe. They test. They find out even where we are at at different parts of the airports, that we take a—quite frankly, a retired senior citizen in Sarasota and do 18 million searches on her, and we are not doing anything on the buses. It is, like, come on.

We really depend on you all to drive us a little bit, because—you are not running right now, and we kind of react when a thing comes, and then we put all the funds in there. But we need to have a balanced thing.

It has been a long time since 9/11 and we still don’t have these kind of core things that we know are high-risk even though, in fact, the Millennium bomber, which would have been the biggest one—if it hadn’t been for an agent at the border on a person who came over on a ferry more or less thinking that the person looked nervous at the end of the day, we could have had an incredible catastrophe.

Mr. WINKOWSKI. I agree. I don’t want to mislead you or the Chairman. I mean, with ferries and trains and buses and small boats, we still do our inspections. I mean, and we still run them through systems.

What I am trying—what we need to do is we have got to, you know, through the risk management models, get that advanced information, make decisions, get rid of that clutter, that low-risk group, spend little time with them and more time with the high-risk.

One of the ways you do that—and we found in the—with advance passenger information is that you are able to make better decisions.

I think also, sir, that I think we have made tremendous inroads since 9/11. I look back at that very unfortunate event and look back at the fact that we never had a National Targeting Center for passenger, and we never had a National Targeting Center for cargo.

We were not advanced from the standpoint of PNR information and APIS information and all the advanced information that we get on the cargo side. We have made tremendous inroads, but I think we have been spending so much time in those areas, on cargo, at the expense of some of these other areas, such as small boats.

I mean, we are spending a lot of intellectual capital here looking at issues like 100 percent scanning when, in fact, we have put in all these layers. I am not saying that it is perfect, but we really need to focus in and I get your message very clearly.

Mr. SOUDER. Let me make it clear. I believe we have made tremendous progress—that we haven’t been attacked. We have had a couple that have misfired, but it is a classic law enforcement—layered things—they make mistakes when they get layered, they are more nervous, they get tipped off, and that sometimes have been

fortunate but most of the time we have stopped them, and that we just cannot flatline here.

The danger is—and the good thing that happened here is it has got everybody concerned again, because we were flatlining. The budget can't flatline either. There are some things that are the clear requirements of the United States Congress to do.

We cannot have county commissioners and State legislators running around trying to figure out how border security is going to work, how we are going to stop terrorists, that when we are working our budget we have to understand which things are clearly our responsibility and which things are shared responsibilities.

We cannot flatline because the challenge is going to get more sophisticated, so we have to keep doing it. But we have made tremendous progress, and I didn't mean to imply that we didn't.

Yield back.

Mr. CUELLAR. Mr. Souder, thank you again very much.

Let me ask you just—suggestions that have been thrown out there that some have argued that visa issuance is no longer a matter of foreign policy but more—primarily it has become a security issue.

Any thoughts on that? I know that is a big change, but any thoughts on that, Mr. Donahue?

Mr. DONAHUE. I think that visa issuance is both. I think that there is a foreign policy aspect to it, but I think it is a security aspect. I think our officers fully understand that in the field. Their first thought in every visa adjudication, No. 1 thought, is how am I protecting my country.

I mentioned that we turned down 2 million visas. We don't know how many of those people were either criminals or terrorists, but in the interview the officer got a funny feeling in his stomach, and—just as the officer did in stopping the Millennium bomber, and said, "This story is not right."

Part of that is being culturally aware. Part of that is speaking in the language of the applicant. Part of that is living in the country, traveling around, knowing—you know yourself. It is hard for people to understand the border situation unless you have lived in the border. I was told that a million times when I served in Mexico.

It is the same thing overseas. We believe that we have an advantage that when we are interviewing, we are—we have this mix of, No. 1, let's keep our country safe, but let's be sure that the vast majority of people who are legitimate travelers, people who are coming here to study in our great universities, people who are coming here to spend their money, people who are investing, that they can get in.

Making that decision takes critical thinking, takes lots of training, and takes a great eye for security.

Mr. CUELLAR. Okay. Thank you.

Mr. Parmer, let's talk about these additional Visa Security Units that ICE plans to stand up this year. What are we doing in the meanwhile while we are waiting to stand those up?

Mr. PARMER. I am sorry, Mr. Chairman, I don't understand your question.

Mr. CUELLAR. In other words, we are planning to put those units in different places across the world. What are we doing in the

meanwhile to address that? Because we are saying that there is a priority to put them in certain places.

What are we doing in the mean time? Do we hope that we get lucky, or what are we doing during that time?

Mr. PARMER. What are we doing toward establishing those offices?

Mr. CUELLAR. Right.

Mr. PARMER. Well, we are selecting the personnel. We are going through the personnel process. We are getting the—looking for housing at post, working with the embassy—

Mr. CUELLAR. While we are going through that process, that absence from that place that you want to set up the unit—nothing—I guess nothing can be done during that time except work through your office.

Mr. DONAHUE. Mr. Chairman, as I said, I was in Mexico last. I had a very close relationship with our ICE colleagues. We stopped people. We revoked visas of people at the advice of ICE. We also depend on the ICE units here in the States that review it. We have other—Department of Homeland Security.

It is a layered approach, and so even in putting this out, we don't know where the next terrorist is going to come from. We have to use smart deployment of all of our skills. They won't be everywhere. But through layered approaches we have a way to cover that.

Mr. CUELLAR. For these units that we want to set up, I know the best thing to do is to have ICE individuals there, because you have got the individuals. What about using some sort of virtual office? Because I am sure there is some resource limitation.

I know that the best thing is to have somebody there. I understand that argument. But in medicine, for example, in Texas we have used telemedicine, where you can have a doctor and, through the telemedicine system, you can see, you can hear, you can talk, you can show him the documentation, you can do everything.

Have you all thought about using that technology to help you expand on a faster basis where you can be domestic but still be able to connect to certain other areas? I know the argument, Mr. Parmer. I know that it is better to have individual. I know that.

But if doctors can do it, there is no reason why law enforcement individuals can't also do that. Any thoughts of using that to at least supplement or at least temporarily use those systems, the technology?

Mr. PARMER. You knew exactly what I was going to say, so I won't belabor that point about the value of having people in country, and it is a similar concept as to why visas aren't issued remotely.

But I think that topic is among those being considered by Assistant Secretary Morton, or some exploration of that topic by Assistant Secretary Morton and his counterpart at State, Assistant Secretary Jacobs.

Mr. CUELLAR. Okay. I would ask you to—and I was just with Secretary Morton last night. I think I am supposed to see him next week again. But I would ask you—and I will tell him, too, but I would ask you all to consider this.

To have somebody there, I understand, it is the best person. But you know, is it better to have somebody or not have anybody at all? At least there is some sort of intermediate system on the technology. The new world that we are in, you know, the systems that we have—I think I would highly, highly encourage you all to at least explore and research this.

You might not be there, but you might have somebody in one of your offices here in the United States be able to work with one of your officers there, one of your employees there, and at least do that.

I mean, I will go back. If doctors can do it through telemedicine, there is no reason why law enforcement—and I know they are different. I understand. I got three brothers who are peace officers, so I understand that.

But I would ask you at least to explore that, so I would ask you to please ask Secretary Morton—I think he is a very innovative, bright individual—that I think you all should at least explore this possibility.

Mr. PARMER. Pardon me, Mr. Donahue.

I just wanted to add that we do have a remote capability that we do work in collaboration with State on, and it is the security advisory opinion process. That does work remotely. You know, again, going back to the—

Mr. CUELLAR. Well, then you got the first step there.

Mr. PARMER. That is right. And—

Mr. CUELLAR. Okay? Okay?

Mr. PARMER. But the value of being able to interact with the applicant, work alongside the consular officers, interact with—liaise with local law enforcement, follow up with family members, business associates, that sort of thing—there is just no replacement for having the ability to do that in country.

Mr. CUELLAR. Right. Well, again, I would highly, highly encourage you to do that.

You know, one of the things that we have seen—and I will use medicine as an example—you might have a doctor there, general practitioner, but then he is able to connect to certain specialist, and that doctor can talk to those specialists who are somewhere else.

If you have certain experts in your office that might not be able to go to some remote part of the world, at least they will be able to connect and talk to—and use the expertise. Nowadays, with this technology, it is like if you are there. Use that. So again, I would strongly ask you to consider that.

I would ask one more thing. What else can we do as Members of Congress, as Congress, to help you all? I will go—Mr. Parmer—and I know you can't go into the budget and ask, because I know you can't lobby us, but—well, what are the more generic things that we can do to help you? I will go one by one.

Mr. PARMER. I am not prepared to answer more of a policy-type question, but I do—I will reiterate our appreciation for the support that you do currently give us. Thank you, Mr. Chairman.

Mr. CUELLAR. Thank you.

I know you are not shy.

Mr. WINKOWSKI. Yeah, Mr. Chairman. We already talked about one. I think we have got to really drill down here on the all modes

APIS. I think it is time, and we have done some preliminary work, and we will certainly work with the staff on that.

Mr. CUELLAR. We were just talking right now, as we talked—what was it, last week, I believe—

Mr. WINKOWSKI. Yes.

Mr. CUELLAR [continuing]. I think we are at that time to start looking at—doing that type of work, so we are going to set up a meeting, a hearing on this particular issue to talk about it, because I still go back—I am a border guy, and I still go back to my numbers.

Eighty-eight percent of the goods or the people coming into United States are coming from land ports. If that is where the majority of the folks coming in, and if I was somebody with bad intentions, I would look at those other areas, whether they are buses—for example, in Laredo, Texas we get about 100 buses a day times, what, 40 individuals.

Just one port, doesn't include California and the other places, just one port in Laredo, 100 buses, 40 individuals, and that gives you an idea. If you do some of that work before they get there, then you can work on the high-risk individuals instead of—everybody across the border on that.

But that doesn't cover ferries and other—

Mr. WINKOWSKI. Not only do you work on the high-risk individuals, of course, with APIS you would set up a system where the—those that need I-94s—they are all printed by the time these individuals come off the bus, or maybe get to a point where they don't even need to come off the bus.

Been down there many times, as you know, and see all these people going into the office, waiting for I-94s to be done. So I think we have got some opportunity there.

Mr. CUELLAR. Right. I want to thank you, because I want you all to continue being forward-thinking. I am glad that the Department is looking at those issues I had. So I appreciate that.

Mr. Donahue, any thoughts?

Mr. DONAHUE. Well, we are extremely grateful for the information-sharing that Congress has encouraged among the agencies. It has changed the way we do business.

We are getting things like the ADIS information, the Arrival and Departure Information System, other systems that are being shared across the Government, and they help our officers in the field.

The one request I would make, partially because we are self-funded, is that we really do encourage you and your Members and your staff members to visit our consular sections.

I think a few minutes—just as you enjoyed at the National Targeting Center, I think a visit to some of our busy visa sections when you are visiting for other business in a capital city or a consular city is a real eye-opening experience to see our officers using the language, protecting our borders, on a daily basis.

Mr. CUELLAR. Yes, sir, and I think that is a very good suggestion.

I want to say thank you to all three of you. Again, I apologize. Sometimes our schedules are beyond our control. Sorry about the delay that we had there. But I really want to thank you all.

I know that your men and women that you all supervise, that you all work with, do a great service to our country, so again, for the State Department, and for ICE and CBP, we really appreciate the good work that you have been doing.

Personally, I feel very—I feel good as to the different improvements that you all have made, because I always look at—we saw what happened, but I am interested in looking forward—what are the lessons learned, what are we learning?—so this doesn't happen again.

Also keep one thing in mind. Mr. Winkowski, we talked about this. We have to be careful about not just relying on the systems themselves. As we mentioned, there is still this sixth sense or this intuition that our men and women have to use, because you just can't look at everything that is on a computer screen.

The more we can encourage this—and I know we talked about that for all the Department. Of course, for ICE and CBP I would ask you to just make sure you tell your folks, you know, to use that sixth sense, if I can use that—as my brothers in law enforcement told me that little sixth sense on that, so I appreciate that.

Again, I would ask you, again, to say—you know, I want to say thank you very much, and I appreciate you all being here. At this time, I want to thank the witnesses for their testimony, Members for their questions.

Again, if there is any additional questions that Members might want to submit, I would ask you to go ahead and submit that to the committee.

Hearing no further business, the subcommittee stands adjourned. Thank you very much.

[Whereupon, at 2:55 p.m., the subcommittee was adjourned.]

