



May 3, 2017

Denying Terrorists Entry to the United States: Examining Visa Security

Subcommittee on Counterterrorism, Committee on Homeland Security,
United States House of Representatives, One Hundred Fifteenth
Congress, First Session

HEARING CONTENTS:

Member Statements

Michael McCaul

[View Statement](#)

Mike Gallagher

[View Statement](#)

Witnesses

Edward Ramotowski
Deputy Assistant Secretary
Office of Visa Services
U.S. Department of State

John Wagner
Deputy Executive Assistant Commissioner
U.S. Customs and Border Protection
U.S. Department of Homeland Security

[View Testimony](#)

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

*This hearing compilation was prepared by the Homeland Security Digital Library,
Naval Postgraduate School, Center for Homeland Defense and Security.*



Michael Dougherty
Acting Assistant Secretary
Border, Immigration, and Trade Policy Office of Policy
U.S. Department of Homeland Security
[View Testimony](#)

Clark E. Settles
Assistant Director
National Security Investigations Division
Immigration and Customs Enforcement
U.S. Department of Homeland Security
[View Testimony](#)

Rebecca Gambler
Director
Homeland Security and Justice
Government Accountability Office
[View Testimony](#)

Available Webcast(s)*:

[Watch Full Hearing](#)

Compiled From*:

<https://homeland.house.gov/hearing/denying-terrorists-entry-united-states-examining-visa-security/>

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

*This hearing compilation was prepared by the Homeland Security Digital Library,
Naval Postgraduate School, Center for Homeland Defense and Security.*



HOMELAND SECURITY COMMITTEE

Statement of Chairman Michael McCaul (R-TX) Task Force on Denying Terrorists Entry to the United States

“Denying Terrorists Entry to the United States: Examining Visa Security”
May 3, 2017

Remarks as Prepared

In June 2000, three of the 9/11 hijackers flew from European cities to Newark International Airport and were admitted into the United States. Their names were Mohamed Atta, Marwan al Shehhi, and Ziad Jarrah. Sadly, we know the rest of the story.

In the years following the 9/11 attacks, the United States government went to great lengths to identify gaps in our vetting systems and in how our agencies share intelligence. The Department of Homeland Security was created by the Bush administration and Congress to help protect America from terrorists by “connecting the dots.”

Now we face a new and growing threat to the homeland. In his speech on April 18, Secretary Kelly described us as a “nation under attack” facing the highest terror threat level in years. Due to our brave service men and women, ISIS and al Qaeda have incurred great losses in Syria and Iraq. Yet as the territory under their control shrinks, we are seeing an exodus of foreign fighters returning to their homelands, 10,000 of which are in Europe.

Our Committee has taken a serious look at foreign fighters. Last Congress, we pulled together a bipartisan Task Force to examine the threat posed to the United States by foreign fighters—especially those traveling in and out of Europe.

Through this extensive, six-month review, the Task Force produced more than 50 actionable recommendations to safeguard the homeland, and this Committee and the House passed legislation to address those recommendations. Those which became law include the Foreign Fighter Travel Review Act, which requires the President to review all Americans who have traveled to Iraq and Syria to join a foreign terrorist organization, and the National Strategy to Combat Terrorist Travel Act, which requires the Administration to develop a substantive strategy to combat the threat posed by extremists and prevent them from entering our country undetected.

Significantly, the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015 ramped up the security of the Visa Waiver Program by improved intelligence information sharing through HSPD-6 agreements and keeps terrorists from entering the United States undetected. It also includes major provisions that will make it harder for terror suspects to cross borders, including enhanced counterterrorism screening of travelers and measures to crack down on passport fraud.

This new Task Force will pick up where the last one left off: addressing the readiness of the homeland in light of the foreign fighter exodus. I was excited to name Congressman Mike Gallagher of Wisconsin as the chair of this initiative. As a former combat veteran and Middle East issue expert, I know he will tackle these urgent issues with seriousness and dedication. Together with the other seven members of this bipartisan Task Force, I know this will be equally productive and essential for America's security.

I look forward to hearing from our witnesses today on the important work performed by DHS and the State Department to prevent terrorists from gaining access to our Homeland.

I yield back the balance of my time.

###



HOMELAND SECURITY COMMITTEE

Statement of Task Force Chairman Mike Gallagher (R-WI) Task Force on Denying Terrorists Entry to the United States

“Denying Terrorists Entry to the United States: Examining Visa Security”
May 3, 2017

Remarks as Prepared

I want to start by welcoming back our expert witnesses to the Capitol and thank them for being here today, as well as for the classified briefing we had yesterday. I look forward to following up on some of the broader themes of the briefing in order to inform the American people of the security of the visa process and the Visa Waiver Program. I also want to thank Chairman McCaul and Ranking Member Thompson for prioritizing this Task Force and its mission.

Last Congress, this Committee’s *Task Force on Combating Terrorist and Foreign Fighter Travel* was not only successful in producing legislative change, but also eye opening in what it revealed. The work done by Members and staff on both sides of the aisle, under Chairman Katko’s leadership, raised awareness about gaps in screening and information sharing—both at home and with our foreign partners—which ultimately led to positive reforms for protecting the homeland against terrorists and foreign fighters. This of course includes the Visa Waiver Program Improvement and Terrorist Travel Prevention Act that enacted major VWP reforms into law in 2015. I hope that this *Task Force on Denying Terrorists Entry into the United States* will be as successful in its investigation and final recommendations. And I look forward to working with Ms. Watson Coleman and all the Members on both sides to ensure that it is a success.

This is a critical time for our nation’s security. The previous task force rightly focused on the tens of thousands of jihadist fighters traveling from the West to join the fight on the ground in Iraq and Syria. Now, however, we see that number dropping as those fighters seek to expand their actions beyond Iraq and Syria. And while coalition forces continue to advance and squeeze ISIS territory, the threat against the West continues to rise as the fighters leave the so-called caliphate. As FBI Director Comey said this past September, “through the fingers of that crush are going to come hundreds of very, very dangerous people...There will be a terrorist diaspora sometime in the next two to five years like we’ve never seen before.”

Those chilling words should serve as a wakeup call. Just last week, it was reported that two British nationals and a U.S. citizen were detained by Turkish border police after spending over two years in ISIS territory. With hundreds of American fighters and thousands of European fighters—armed with lawful passports, terrorist training, and jihadist connections—seeking to return to their home countries, we must be able to prevent them from gaining entry into the United States by abusing our immigration system. ISIS has already planned, conducted, or inspired more than 180 plots against the West, including the 2015 attacks in Paris, and the 2016 attacks in Brussels, Nice, and Berlin. The majority of these attackers were European citizens with valid passports, so it is easy to imagine any one of them gaining access to this country through a valid visa or through the Visa Waiver Program. And as Secretary Kelly recently said, the U.S. is “the prime

terrorist target,” especially since so many of these fighters are citizens of VWP countries. But that is why we are here today—to ensure that our defenses are strong and to protect the Homeland as it continues to be targeted.

While there are numerous benefits to our country that stem from our welcoming immigration system—like tourism, trade, and business—we should never cease to examine our processes through the lens of a terrorist in search potential gaps. We must always strive to stay one step ahead. That is what we learned in the wake of September 11th, where all of the attackers entered the U.S. through legal means, mainly through lawful tourist visas. This of course prompted an overhaul of our immigration and transportation security systems, as well as the creation of the Department of Homeland Security. But our work is not done. We still have a lot to learn and adapt to.

Despite the reforms undertaken in the wake of 9/11, there are still gaps and weaknesses in our system. One of the attackers who killed 14 people in San Bernardino in 2015 legally entered into this country on a K-1 “fiancé” visa—raising questions on the level of scrutiny given to visa applications. There are also remaining gaps in vetting and screening of VWP applicants, and in information sharing with other countries, which are both vital in the fight against the terrorist diaspora.

I look forward to hearing from our expert witnesses on what the Department of Homeland Security and the Department of State are doing to ensure that visa and VWP applicants are receiving sufficient screening and vetting before they are allowed to enter into this country. I thank the witnesses for being here and for their service—as well as the many men and women who serve our nation at both DHS and the State Department.

###



TESTIMONY OF

MICHAEL DOUGHERTY

Acting Assistant Secretary for Border, Immigration, and Trade
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security

JOHN WAGNER

Deputy Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection
Department of Homeland Security

CLARK E. SETTLES

Assistant Director, National Security Investigations
U.S. Immigration and Customs Enforcement
Department of Homeland Security

BEFORE THE

U.S. House of Representatives

Committee on Homeland Security
Taskforce on Denying Terrorist Entry into the United States

ON

Denying Terrorists Entry to the United States: Examining Visa Security

May 3, 2017
Washington, DC

Introduction

Chairman Gallagher, Ranking Member Watson Coleman, and distinguished Committee Members.

Thank you for the opportunity to appear before you today to discuss the efforts of the Department of Homeland Security (DHS) to prevent terrorists and other criminal actors from entering the United States, either by acquiring U.S. visas or traveling through the Visa Waiver Program (VWP). This work involves close interagency collaboration and partnership with foreign governments. Ultimately, traveler screening and vetting is an integral component of our responsibility to protect the homeland, and DHS employs a multi-layered strategy to do so.

Furthermore, as called for in Section 5 of the President's Executive Order (EO) 13780, *Protecting The Nation From Foreign Terrorist Entry Into The United States*, DHS is diligently working with the Departments of State (DOS) and Justice and the Office of the Director of National Intelligence (ODNI) to implement a uniform baseline for screening and vetting standards and procedures. These standards seek "to identify individuals who seek to enter the United States on a fraudulent basis, who support terrorism, violent extremism, acts of violence toward any group or class of people within the United States, or who present a risk of causing harm subsequent to their entry."

DHS Secretary John F. Kelly has made clear that blocking terrorists and criminals from accessing the United States is one of his highest priorities, and the Administration is undertaking serious and sustained efforts to ensure that we keep bad actors from reaching our shores and endangering our people. As part of this effort, we are modernizing screening, expanding information sharing within our government and with foreign partners, and exploring innovative approaches for detecting threat actors. By focusing on better obstructing terrorists and criminals, we can more effectively facilitate legitimate trade and travel.

Pushing Out the Zone of Security

Secretary Kelly noted in his remarks at George Washington University on April 18, 2017, that "[t]he more we push our borders out, the safer our homeland will be." The Secretary went on to highlight in those remarks the importance of knowing who is coming into the country and what their intent for coming is prior to their arrival "at our doorstep." There are a multitude of activities, efforts, and programs that DHS and its Component Agencies undertake to do just that.

In Fiscal Year (FY) 2016, U.S Customs and Border Protection (CBP) inspected over 390 million travelers at 328 ports of entry (POE), of which over 119 million flew into air POEs. CBP's pre-departure strategy is one of the ways by which DHS assists our interagency, foreign government, and private sector partners to deny international travel to potential terrorists and criminals. A major component of this strategy is the recommendation of denial of visas, as well as denial and/or revocation of visa waiver approvals to individuals who may present a risk to national security or public safety. It is a risk-based, intelligence-driven strategy that extends our border security efforts outward to detect, assess, and mitigate, at the earliest possible point in the travel continuum, any risk posed by travelers before they reach the United States. As threats evolve,

CBP works in close partnership with our foreign counterparts – including those in Europe, North Africa, and the Middle East – to develop greater situational awareness of emerging threats, leverage partner capabilities to affect threat networks, and coordinate enforcement actions. These concerns are not limited to the United States and there is a growing international commitment to combating these shared threats to our security.

U.S. Immigration and Customs Enforcement (ICE) also actively works to push our defenses outward. To achieve this goal, ICE forward deploys personnel to 66 offices in 49 countries. ICE’s international staff works in conjunction with overseas law enforcement counterparts to detect, disrupt, and dismantle transnational criminal groups and individuals who seek to harm our country and people. Furthermore, ICE special agents investigate transnational crime by conducting a wide range of criminal investigations in coordination with our foreign and domestic partner agencies, targeting the illegal movement of people, merchandise and monetary instruments into, within, and out of the United States.

Visa and Travel Authorization Security

As President Trump has stated, “Homeland Security is in the business of saving lives, and that mandate will guide our actions.” Since taking office this Administration has worked tirelessly to enhance border security, promote public safety, and minimize the threat of terrorist attacks by foreign nationals in the United States. Part of this process is ensuring the security of international travel by preventing dangerous persons from obtaining visas, travel authorizations, and boarding passes. Before boarding a flight or vessel destined for the United States, most foreign nationals must obtain a non-immigrant visa from the DOS — issued at a U.S. Embassy or Consulate. The visa process involves multiple security checks, including screening of applicants against a wide array of criminal and terrorist databases to verify the individual’s identity and to detect derogatory information that might lead to an inadmissibility determination, as well as an in-person interview with the applicant.

CBP also conducts vetting of all valid immigrant and non-immigrant visas. Although the visa application and adjudication processes rest with the DOS, CBP’s National Targeting Center (NTC) conducts continuous vetting of U.S. immigrant and nonimmigrant visas that have been recently issued or revoked. Recurrent vetting ensures that changes in a traveler’s admissibility and eligibility for travel are identified in near real-time, allowing CBP to immediately determine if it is necessary to take action prior to subject’s arrival to the United States, such as a “no board” recommendation to a carrier, and/or a recommendation to the DOS to revoke the visa.

In an effort to augment and expand visa security operations, ICE manages the Visa Security Program (VSP) for DHS. VSP’s primary purpose is to identify terrorists, criminals, and other individuals who pose a threat or are otherwise ineligible for visas prior to visa adjudication or application for admission to the United States. VSP operations are currently conducted at 30 visa-issuing posts in 25 countries.

Through the VSP, ICE deploys special agents to visa issuing posts worldwide to utilize available investigative resources, in-person interviews, and collaboration between U.S. agencies and our foreign counterparts, in order to investigate and disrupt the travel of suspect individuals during

the visa application process. Experience has shown the Department that there is no technological substitute for having experienced ICE special agents deployed overseas to apply law enforcement capabilities to the visa process through investigative measures, informed interviews with suspect applicants, and leveraging local contacts for information.

Special Agents assigned to international VSP posts are supported through domestic-based screening and vetting of visa applicants, the Pre-Adjudicated Threat Recognition and Intelligence Operations Team (PATRIOT). PATRIOT is an interagency endeavor between ICE and CBP's NTC. Through PATRIOT, VSP conducts automated screening of visa application information against DHS holdings, as well as holdings of other U.S. agencies, prior to the visa applicant's interview and visa adjudication. Derogatory information discovered during automated screening is manually vetted and analyzed by domestic PATRIOT personnel using law enforcement, open source, and classified information. PATRIOT analysts then provide deployed VSP personnel with relevant information prior to interviews and other investigative activities. Following an analysis of all known derogatory information, deployed ICE special agents provide a unified DHS recommendation on visa eligibility to DOS consular officers.

In FY 2016, VSP deployed special agents and PATRIOT personnel facilitated the screening and vetting of more than 2.2 million visa applicants, recommended the refusal of more than 8,500 visas, and submitted 1,669 Terrorist Screening Center Database nominations. The VSP will expand to two additional posts in FY 2017 and is tentatively scheduled to add an additional two posts in FY 2018.

If travelers are eligible to travel under the VWP, they must apply for and be approved for a travel authorization via the Electronic System for Travel Authorization (ESTA). Through ESTA, CBP conducts enhanced vetting of potential VWP travelers to assess whether they are eligible to travel under the VWP or could pose a risk to the United States or the public at large. All ESTA applications are screened against security and law enforcement databases, and CBP automatically refuses authorization to individuals who are found to be ineligible to travel to the United States under the VWP. Similarly, current and valid ESTAs may be revoked if concerns arise through recurrent vetting.¹

In November 2016, CBP launched the Electronic Visa Update System (EVUS). Similar to ESTA, EVUS is an online system used by visa holders to periodically update their biographic information to facilitate their travel to the United States.² To maintain a valid visa for purposes of seeking admission to the United States, travelers with designated nonimmigrant visas from identified countries are required to maintain a valid EVUS enrollment before travelling to the United States. Enrollments generally last for two years or when the traveler's visa or passport expires, whichever comes first. Data collected through EVUS helps us determine whether such travel poses a law enforcement or security risk by checking against select law enforcement

¹ Recurrent vetting is ongoing throughout the period of validity of the ESTA. ESTA applicants who are denied may apply for a nonimmigrant visa.

² At this time, EVUS is only a requirement for individuals travelling on passports issued by the People's Republic of China who have been issued unrestricted, maximum validity B-1 (visitor for business) or B-2 (visitor for pleasure) visas, generally valid for 10 years, Chinese nationals. The requirement is new, and the U.S. Government expects that it may be applied to additional countries or nonimmigrant categories may be designated in the future.

databases and queries law enforcement databases that include terrorist screening, lost/stolen passports, INTERPOL wants/warrants, and immigration violations.

Finally, thanks to the support of Congress, the *Department of Homeland Security Appropriations Act of 2015*³ provided the necessary funds for CBP to initiate counter-network operations within the NTC. The newly-established Counter Network Division's (CND) mission supports CBP, other DHS Components, and interagency law enforcement and Intelligence Community partners to develop an interoperable counter-network process that provides a comprehensive understanding of emerging threats, including those emanating from terrorism, special interest aliens, transnational organized crime and illicit trade networks. Informed through identification of the tactics, techniques, and procedures of adversarial networks – including their efforts to exploit legitimate travel pathways and processes such as the visa process and the VWP – the CND quickly develops analytic solutions and makes those available across DHS components to mitigate further risk.

Visa Waiver Program

An important way in which DHS is pushing out the zone of security is to work with our international partners, including those countries who are members of the VWP. DHS's focus and priority for the VWP is to make it a comprehensive security partnership with America's closest allies. The VWP must be a security program first and foremost—merging together best practices in national security, law enforcement security, and immigration security; and providing the United States with an effective tool for fostering and deepening our national security relationships with key partner countries. As Secretary Kelly recently indicated, we have to continue to look at ways to strengthen the security of the VWP given the threat of foreign fighters returning from the battlefields of Syria and Iraq. DHS is committed to fully ensuring that the VWP is serving the security interests of the United States.

Currently, 38 countries^{4,5} participate in the VWP, which allows their nationals to travel to the United States for business or tourism for stays of up to 90 days (with certain exceptions) after applying and being approved through the ESTA.⁶ In return, these countries must prove that measurable and consistently high requirements are met, including: that information sharing practices enable the rapid relay of information concerning known and suspected terrorists and serious criminals; that lost and stolen passport information is consistently and timely reported; that robust border and travel document security practices are in place; and that effective traveler and migrant screening practices are standard operations. VWP countries also undergo regular,

³ Pub.L. No. 114-4.

⁴ VWP-eligible countries: Andorra, Australia, Austria, Belgium, Brunei, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, The Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, Taiwan, United Kingdom.

⁵ Per the Taiwan Relations Act of 1979, all references to “country” or “countries” in this document also apply with respect to Taiwan.

⁶ Exceptions include citizens of countries under other visa exempt authority, such as Canada. Citizens of countries under visa exempt authority traveling to entering the United States via air are subjected to CBP's vetting and inspection processes prior to their departure for the United States. In the land environment, they are subject to CBP processing upon arrival at a U.S. port of entry.

in-depth security assessments conducted by DHS in consultation with DOS to ensure compliance with these requirements.

The assessments of a VWP country's security standards and operations are among the broadest and most consequential reviews conducted under any U.S. Government program. Rigorous national-level assessments are used to ensure that countries meet the security standards required for continued participation in the Program. DHS, in coordination with the DOS and the Intelligence Community, conducts statutorily-required reviews of each VWP country at least once every two years. The VWP assessment evaluates the country's counterterrorism and law enforcement capabilities, immigration enforcement policies and procedures, passport production and issuance processes, and border security traveler screening capabilities. As needed, the review may also include a site visit where an integrated U.S. Government team conducts thorough inspections of airports, seaports, land borders, and passport production and issuance facilities in the VWP country and holds discussions with the host government, counterterrorism, intelligence, law enforcement, border security, and immigration officials. DHS submits a Report to Congress upon the completion of the assessment. Notably, both the Government Accountability Office (GAO) and the DHS Office of the Inspector General (OIG) have reviewed and written favorably of the methodology DHS uses in conducting these assessments.⁷

Separately, DHS also conducts an annual assessment of all 38 VWP countries against the risk criteria defined in the *Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015* (VWP Improvement Act), passed under this Committee's leadership, and engages in ongoing monitoring of member countries to rapidly identify emerging threats and vulnerabilities.

The bottom line is that in order to join or continue in the VWP, a country cannot represent a threat to the United States and must be working as a partner to prevent terrorist travel. In all instances, the Secretary of Homeland Security retains the statutory authority to suspend or terminate a country's participation in the VWP if there is a credible threat originating from that country that poses an imminent danger to the United States or its citizens.

Under the VWP Improvement Act, VWP countries are now required to issue high-security electronic passports (e-passports); implement information sharing arrangements to exchange criminal and terrorist identity information; establish mechanisms to validate e-passports at each key POE; report all lost and stolen passports to INTERPOL or directly to the United States no later than 24 hours after the country becomes aware of the loss or theft; conclude a U.S. Federal Air Marshals agreement; collect and analyze Advance Passenger Information (API)/Passenger Name Record (PNR) information to identify high-risk travelers; screen international travelers against the INTERPOL Stolen and Lost Travel Documents (SLTD) database and notices; report foreign fighters to multilateral security organizations, such as INTERPOL or EUROPOL; and cooperate with the United States in the screening of refugees and asylum seekers.

Since passage of the Act, DHS has confirmed the following changes among VWP countries:

- An increase in the sharing of terrorist and criminal identity information;

⁷ DHS report OIG-13-07 "The Visa Waiver Program," November 2012. GAO report GAO-16-498 "Visa Waiver Program," May 2016.

- Several countries⁸ have increased the frequency of their reporting of lost and stolen passports — VWP countries account for over 70 percent of the almost 73 million lost and stolen travel documents reported to INTERPOL;
- Several countries have agreed to adopt new technologies to work with DHS to jointly vet asylum, refugee, and other immigration applications against each other's data, establishing a formidable force multiplier for detecting criminals, terrorists and unqualified applicants; and
- All VWP countries are now issuing and using for travel to the United States fraud-resistant e-passports that meet or exceed the International Civil Aviation Organization standards.

In addition, following the enactment of the VWP Improvement Act, DHS has taken several steps to apply enhanced restrictions on visa-free travel under the VWP for individuals who have traveled to Iran, Iraq, Sudan, Syria, Libya, Somalia, or Yemen or individuals who are dual nationals of Iran, Iraq, Sudan or Syria. Beginning January 13, 2016, CBP initiated a protocol to identify ESTA holders who had travelled to Iraq, Syria, Iran, or Sudan since March 1, 2011 who may be ineligible for future travel if they do not meet the criteria for a waiver allowed for under the Act. On February 18, 2016, DHS announced that individuals who had travelled to Libya, Somalia, and Yemen also may be ineligible for future travel if they do not meet the criteria for a waiver.⁹ Additionally, on January 21, 2016, CBP began denying new ESTA applications and revoking existing ESTAs for individuals who indicated dual nationality with Iran, Iraq, Sudan, or Syria.

In November 2014, in response to increasing concerns regarding foreign terrorist fighters, DHS strengthened the security of the VWP through the addition of new data elements to the ESTA application. These enhancements included a series of additional questions a VWP traveler must answer on the ESTA application, to include other names/aliases, citizenships, contact information, and city of birth.

Arrival Processing

CBP's use of advance information, its pre-departure targeting operations, and its overseas footprint all comprise critical parts of CBP's multi-layered security strategy to address concerns long before they reach the physical border of the United States. U.S. law requires all private and commercial air and sea carriers operating routes to, from, or through the United States to provide API and PNR data to CBP. These data, which include travelers' biographic and travel reservation information, are screened against U.S. and international law enforcement and counterterrorism databases to identify high-risk individuals before they fly to the United States. Even if issued a visa or other travel authorization, however, it is important to note that upon arrival in the United States, all persons are subject to inspection by CBP Officers. CBP Officers review entry documents, query CBP and other law enforcement databases, collect biometrics

⁸ Including Brunei, Greece, Hungary, and Portugal.

⁹In FY 2016, since implementing the new travel and dual nationality restrictions to the Visa Waiver Program, CBP denied, canceled, or revoked 39,303 ESTA applications. These individuals would not be eligible to travel under the VWP.

(including from VWP travelers),¹⁰ and interview all travelers to determine the purpose and intent of their travel, and whether any further inspection is necessary based on, among other things, national security, admissibility, customs, or agriculture concerns.

Of note, CBP's Tactical Terrorism Response Teams (TTRT) are deployed at U.S. POEs and consist of CBP Officers who are specially trained in counterterrorism response. TTRT Officers utilize information derived from targeting and inspection to mitigate possible threats. TTRT officers are immersed in the current and developing threat picture through the continuous review of information, and are responsible for the examination of travelers identified within the Terrorist Screening Database, and other travelers suspected of having a nexus to terrorism who arrive to a POE. For FY 2017 to date¹¹, as a result of the dedicated efforts of the men and women serving on CBP's TTRT, and the information discovered during secondary inspection, nearly 600 people who had been granted visas or other travel documents, or had an approved ESTA, have been refused admission to the United States. CBP Officers and Agents remain our last line of defense against those who would seek to enter the country to do us harm.

In addition, CBP Officers remove from circulation counterfeit, fraudulent, and altered travel documents, as well as lost or stolen travel documents presented for use by an individual other than the rightful holder, such as those presented by impostors. CBP currently uses 1:1 facial comparison technology at select primary lanes at John F. Kennedy International Airport and Washington Dulles International Airport on U.S. and non-U.S. travelers arriving in the United States. This technology enables CBP Officers to use facial recognition technology as a tool to assist in determining whether an individual presenting a valid e-passport is the same individual whose photograph is contained in that passport. In those cases where the CBP Officer is unsure of the traveler's true identity, the traveler is referred for additional checks to confirm identity or to document fraudulent use of a passport. Since this technology was deployed in early 2016, over 400,000 travelers have had their identities confirmed with the use of 1:1 facial comparison technology.

Finally, CBP's Fraudulent Document Analysis Unit (FDAU) serves as the central repository and point of analysis for all fraudulent travel documents interdicted or recovered by CBP personnel. FDAU analysis of fraudulent documents provides intelligence, alerts and training back to the field, as well as serves as a mechanism to remove fraudulent documents from circulation to prevent their further use – a lesson learned from the 9/11 Commission Report. This cyclical process adds a layer of security to the homeland by removing an additional opportunity for misuse.

Identifying and Apprehending Threats to National Security and Public Safety within the United States

An important mission of DHS is to actively identify and initiate enforcement action on persons who have overstayed their terms of admission in the United States and who pose a threat to national security, border security, or public safety. ICE undertakes this very important activity for DHS. Within ICE, there are dedicated units, special agents, analysts, and systems in place to

¹⁰ Biometrics are collected for most foreign nationals arriving at U.S. airports.

¹¹ As of April 19, 2017

address nonimmigrant overstays. Through investigative efforts, ICE analyzes and determines which overstay leads may be suitable for further national security investigation. Once leads are received, ICE conducts both batch and manual vetting against government databases, public indices, and social media (when appropriate). This vetting helps determine if an individual who overstayed has departed the United States, adjusted to a lawful status, has a pending immigration benefit application, or would be appropriate for an enforcement action.

As part of this tiered review, ICE prioritizes nonimmigrant overstay cases through risk-based analysis. ICE Homeland Security Investigation's (HSI) Counterterrorism and Criminal Exploitation Unit (CTCEU) oversees the national program dedicated to the investigation of nonimmigrant visa violators who may pose a national security risk and/or public safety concern. Each year, CTCEU analyzes records of hundreds of thousands of potential status violators after preliminary analysis of data from various government systems, including the Student and Exchange Visitor Information System (SEVIS) and CBP's Arrival and Departure Information System (ADIS), along with other information. After this analysis, CTCEU establishes compliance or departure dates from the United States and/or determines potential violations that warrant field investigations.

CTCEU proactively develops cases for investigation in furtherance of the overstay mission, monitors the latest threat reports, and addresses emergent issues. This practice, which is designed to detect and identify individuals exhibiting specific risk factors based on intelligence reporting, travel patterns, and in-depth criminal research and analysis, has contributed to DHS's counterterrorism mission by initiating and supporting high-priority national security initiatives based on specific intelligence.

In FY 2015, CTCEU reviewed 971,305 leads regarding potential overstays. Numerous leads were closed through an automated screening and vetting process. The most common reason for closure was subsequent departure from the United States. A total of 9,968 leads were sent to HSI field offices for investigation. As a result in FY 2015 alone, HSI made 1,910 arrests, secured 86 indictments, and obtained 80 convictions.

CTCEU refers leads that do not meet ICE HSI criteria for further investigation to ICE Enforcement and Removal Operations' National Criminal Analysis and Targeting Center.

Conclusion

The men and women of DHS and its Component Agencies do a tremendous job every day to protect our country. As terrorists and criminals change their methods and tactics and technologies continue to evolve, DHS will work with its interagency and foreign partners— as well as private sector partners — to adapt and respond swiftly and effectively to prevent their entry into the United States.

Thank you again for the opportunity to testify today. We look forward to answering your questions.



TESTIMONY OF

MICHAEL DOUGHERTY

Acting Assistant Secretary for Border, Immigration, and Trade
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security

JOHN WAGNER

Deputy Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection
Department of Homeland Security

CLARK E. SETTLES

Assistant Director, National Security Investigations
U.S. Immigration and Customs Enforcement
Department of Homeland Security

BEFORE THE

U.S. House of Representatives

Committee on Homeland Security
Taskforce on Denying Terrorist Entry into the United States

ON

Denying Terrorists Entry to the United States: Examining Visa Security

May 3, 2017
Washington, DC

Introduction

Chairman Gallagher, Ranking Member Watson Coleman, and distinguished Committee Members.

Thank you for the opportunity to appear before you today to discuss the efforts of the Department of Homeland Security (DHS) to prevent terrorists and other criminal actors from entering the United States, either by acquiring U.S. visas or traveling through the Visa Waiver Program (VWP). This work involves close interagency collaboration and partnership with foreign governments. Ultimately, traveler screening and vetting is an integral component of our responsibility to protect the homeland, and DHS employs a multi-layered strategy to do so.

Furthermore, as called for in Section 5 of the President's Executive Order (EO) 13780, *Protecting The Nation From Foreign Terrorist Entry Into The United States*, DHS is diligently working with the Departments of State (DOS) and Justice and the Office of the Director of National Intelligence (ODNI) to implement a uniform baseline for screening and vetting standards and procedures. These standards seek "to identify individuals who seek to enter the United States on a fraudulent basis, who support terrorism, violent extremism, acts of violence toward any group or class of people within the United States, or who present a risk of causing harm subsequent to their entry."

DHS Secretary John F. Kelly has made clear that blocking terrorists and criminals from accessing the United States is one of his highest priorities, and the Administration is undertaking serious and sustained efforts to ensure that we keep bad actors from reaching our shores and endangering our people. As part of this effort, we are modernizing screening, expanding information sharing within our government and with foreign partners, and exploring innovative approaches for detecting threat actors. By focusing on better obstructing terrorists and criminals, we can more effectively facilitate legitimate trade and travel.

Pushing Out the Zone of Security

Secretary Kelly noted in his remarks at George Washington University on April 18, 2017, that "[t]he more we push our borders out, the safer our homeland will be." The Secretary went on to highlight in those remarks the importance of knowing who is coming into the country and what their intent for coming is prior to their arrival "at our doorstep." There are a multitude of activities, efforts, and programs that DHS and its Component Agencies undertake to do just that.

In Fiscal Year (FY) 2016, U.S Customs and Border Protection (CBP) inspected over 390 million travelers at 328 ports of entry (POE), of which over 119 million flew into air POEs. CBP's pre-departure strategy is one of the ways by which DHS assists our interagency, foreign government, and private sector partners to deny international travel to potential terrorists and criminals. A major component of this strategy is the recommendation of denial of visas, as well as denial and/or revocation of visa waiver approvals to individuals who may present a risk to national security or public safety. It is a risk-based, intelligence-driven strategy that extends our border security efforts outward to detect, assess, and mitigate, at the earliest possible point in the travel continuum, any risk posed by travelers before they reach the United States. As threats evolve,

CBP works in close partnership with our foreign counterparts – including those in Europe, North Africa, and the Middle East – to develop greater situational awareness of emerging threats, leverage partner capabilities to affect threat networks, and coordinate enforcement actions. These concerns are not limited to the United States and there is a growing international commitment to combating these shared threats to our security.

U.S. Immigration and Customs Enforcement (ICE) also actively works to push our defenses outward. To achieve this goal, ICE forward deploys personnel to 66 offices in 49 countries. ICE’s international staff works in conjunction with overseas law enforcement counterparts to detect, disrupt, and dismantle transnational criminal groups and individuals who seek to harm our country and people. Furthermore, ICE special agents investigate transnational crime by conducting a wide range of criminal investigations in coordination with our foreign and domestic partner agencies, targeting the illegal movement of people, merchandise and monetary instruments into, within, and out of the United States.

Visa and Travel Authorization Security

As President Trump has stated, “Homeland Security is in the business of saving lives, and that mandate will guide our actions.” Since taking office this Administration has worked tirelessly to enhance border security, promote public safety, and minimize the threat of terrorist attacks by foreign nationals in the United States. Part of this process is ensuring the security of international travel by preventing dangerous persons from obtaining visas, travel authorizations, and boarding passes. Before boarding a flight or vessel destined for the United States, most foreign nationals must obtain a non-immigrant visa from the DOS — issued at a U.S. Embassy or Consulate. The visa process involves multiple security checks, including screening of applicants against a wide array of criminal and terrorist databases to verify the individual’s identity and to detect derogatory information that might lead to an inadmissibility determination, as well as an in-person interview with the applicant.

CBP also conducts vetting of all valid immigrant and non-immigrant visas. Although the visa application and adjudication processes rest with the DOS, CBP’s National Targeting Center (NTC) conducts continuous vetting of U.S. immigrant and nonimmigrant visas that have been recently issued or revoked. Recurrent vetting ensures that changes in a traveler’s admissibility and eligibility for travel are identified in near real-time, allowing CBP to immediately determine if it is necessary to take action prior to subject’s arrival to the United States, such as a “no board” recommendation to a carrier, and/or a recommendation to the DOS to revoke the visa.

In an effort to augment and expand visa security operations, ICE manages the Visa Security Program (VSP) for DHS. VSP’s primary purpose is to identify terrorists, criminals, and other individuals who pose a threat or are otherwise ineligible for visas prior to visa adjudication or application for admission to the United States. VSP operations are currently conducted at 30 visa-issuing posts in 25 countries.

Through the VSP, ICE deploys special agents to visa issuing posts worldwide to utilize available investigative resources, in-person interviews, and collaboration between U.S. agencies and our foreign counterparts, in order to investigate and disrupt the travel of suspect individuals during

the visa application process. Experience has shown the Department that there is no technological substitute for having experienced ICE special agents deployed overseas to apply law enforcement capabilities to the visa process through investigative measures, informed interviews with suspect applicants, and leveraging local contacts for information.

Special Agents assigned to international VSP posts are supported through domestic-based screening and vetting of visa applicants, the Pre-Adjudicated Threat Recognition and Intelligence Operations Team (PATRIOT). PATRIOT is an interagency endeavor between ICE and CBP's NTC. Through PATRIOT, VSP conducts automated screening of visa application information against DHS holdings, as well as holdings of other U.S. agencies, prior to the visa applicant's interview and visa adjudication. Derogatory information discovered during automated screening is manually vetted and analyzed by domestic PATRIOT personnel using law enforcement, open source, and classified information. PATRIOT analysts then provide deployed VSP personnel with relevant information prior to interviews and other investigative activities. Following an analysis of all known derogatory information, deployed ICE special agents provide a unified DHS recommendation on visa eligibility to DOS consular officers.

In FY 2016, VSP deployed special agents and PATRIOT personnel facilitated the screening and vetting of more than 2.2 million visa applicants, recommended the refusal of more than 8,500 visas, and submitted 1,669 Terrorist Screening Center Database nominations. The VSP will expand to two additional posts in FY 2017 and is tentatively scheduled to add an additional two posts in FY 2018.

If travelers are eligible to travel under the VWP, they must apply for and be approved for a travel authorization via the Electronic System for Travel Authorization (ESTA). Through ESTA, CBP conducts enhanced vetting of potential VWP travelers to assess whether they are eligible to travel under the VWP or could pose a risk to the United States or the public at large. All ESTA applications are screened against security and law enforcement databases, and CBP automatically refuses authorization to individuals who are found to be ineligible to travel to the United States under the VWP. Similarly, current and valid ESTAs may be revoked if concerns arise through recurrent vetting.¹

In November 2016, CBP launched the Electronic Visa Update System (EVUS). Similar to ESTA, EVUS is an online system used by visa holders to periodically update their biographic information to facilitate their travel to the United States.² To maintain a valid visa for purposes of seeking admission to the United States, travelers with designated nonimmigrant visas from identified countries are required to maintain a valid EVUS enrollment before travelling to the United States. Enrollments generally last for two years or when the traveler's visa or passport expires, whichever comes first. Data collected through EVUS helps us determine whether such travel poses a law enforcement or security risk by checking against select law enforcement

¹ Recurrent vetting is ongoing throughout the period of validity of the ESTA. ESTA applicants who are denied may apply for a nonimmigrant visa.

² At this time, EVUS is only a requirement for individuals travelling on passports issued by the People's Republic of China who have been issued unrestricted, maximum validity B-1 (visitor for business) or B-2 (visitor for pleasure) visas, generally valid for 10 years, Chinese nationals. The requirement is new, and the U.S. Government expects that it may be applied to additional countries or nonimmigrant categories may be designated in the future.

databases and queries law enforcement databases that include terrorist screening, lost/stolen passports, INTERPOL wants/warrants, and immigration violations.

Finally, thanks to the support of Congress, the *Department of Homeland Security Appropriations Act of 2015*³ provided the necessary funds for CBP to initiate counter-network operations within the NTC. The newly-established Counter Network Division's (CND) mission supports CBP, other DHS Components, and interagency law enforcement and Intelligence Community partners to develop an interoperable counter-network process that provides a comprehensive understanding of emerging threats, including those emanating from terrorism, special interest aliens, transnational organized crime and illicit trade networks. Informed through identification of the tactics, techniques, and procedures of adversarial networks – including their efforts to exploit legitimate travel pathways and processes such as the visa process and the VWP – the CND quickly develops analytic solutions and makes those available across DHS components to mitigate further risk.

Visa Waiver Program

An important way in which DHS is pushing out the zone of security is to work with our international partners, including those countries who are members of the VWP. DHS's focus and priority for the VWP is to make it a comprehensive security partnership with America's closest allies. The VWP must be a security program first and foremost—merging together best practices in national security, law enforcement security, and immigration security; and providing the United States with an effective tool for fostering and deepening our national security relationships with key partner countries. As Secretary Kelly recently indicated, we have to continue to look at ways to strengthen the security of the VWP given the threat of foreign fighters returning from the battlefields of Syria and Iraq. DHS is committed to fully ensuring that the VWP is serving the security interests of the United States.

Currently, 38 countries^{4,5} participate in the VWP, which allows their nationals to travel to the United States for business or tourism for stays of up to 90 days (with certain exceptions) after applying and being approved through the ESTA.⁶ In return, these countries must prove that measurable and consistently high requirements are met, including: that information sharing practices enable the rapid relay of information concerning known and suspected terrorists and serious criminals; that lost and stolen passport information is consistently and timely reported; that robust border and travel document security practices are in place; and that effective traveler and migrant screening practices are standard operations. VWP countries also undergo regular,

³ Pub.L. No. 114-4.

⁴ VWP-eligible countries: Andorra, Australia, Austria, Belgium, Brunei, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, The Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, Taiwan, United Kingdom.

⁵ Per the Taiwan Relations Act of 1979, all references to “country” or “countries” in this document also apply with respect to Taiwan.

⁶ Exceptions include citizens of countries under other visa exempt authority, such as Canada. Citizens of countries under visa exempt authority traveling to entering the United States via air are subjected to CBP's vetting and inspection processes prior to their departure for the United States. In the land environment, they are subject to CBP processing upon arrival at a U.S. port of entry.

in-depth security assessments conducted by DHS in consultation with DOS to ensure compliance with these requirements.

The assessments of a VWP country's security standards and operations are among the broadest and most consequential reviews conducted under any U.S. Government program. Rigorous national-level assessments are used to ensure that countries meet the security standards required for continued participation in the Program. DHS, in coordination with the DOS and the Intelligence Community, conducts statutorily-required reviews of each VWP country at least once every two years. The VWP assessment evaluates the country's counterterrorism and law enforcement capabilities, immigration enforcement policies and procedures, passport production and issuance processes, and border security traveler screening capabilities. As needed, the review may also include a site visit where an integrated U.S. Government team conducts thorough inspections of airports, seaports, land borders, and passport production and issuance facilities in the VWP country and holds discussions with the host government, counterterrorism, intelligence, law enforcement, border security, and immigration officials. DHS submits a Report to Congress upon the completion of the assessment. Notably, both the Government Accountability Office (GAO) and the DHS Office of the Inspector General (OIG) have reviewed and written favorably of the methodology DHS uses in conducting these assessments.⁷

Separately, DHS also conducts an annual assessment of all 38 VWP countries against the risk criteria defined in the *Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015* (VWP Improvement Act), passed under this Committee's leadership, and engages in ongoing monitoring of member countries to rapidly identify emerging threats and vulnerabilities.

The bottom line is that in order to join or continue in the VWP, a country cannot represent a threat to the United States and must be working as a partner to prevent terrorist travel. In all instances, the Secretary of Homeland Security retains the statutory authority to suspend or terminate a country's participation in the VWP if there is a credible threat originating from that country that poses an imminent danger to the United States or its citizens.

Under the VWP Improvement Act, VWP countries are now required to issue high-security electronic passports (e-passports); implement information sharing arrangements to exchange criminal and terrorist identity information; establish mechanisms to validate e-passports at each key POE; report all lost and stolen passports to INTERPOL or directly to the United States no later than 24 hours after the country becomes aware of the loss or theft; conclude a U.S. Federal Air Marshals agreement; collect and analyze Advance Passenger Information (API)/Passenger Name Record (PNR) information to identify high-risk travelers; screen international travelers against the INTERPOL Stolen and Lost Travel Documents (SLTD) database and notices; report foreign fighters to multilateral security organizations, such as INTERPOL or EUROPOL; and cooperate with the United States in the screening of refugees and asylum seekers.

Since passage of the Act, DHS has confirmed the following changes among VWP countries:

- An increase in the sharing of terrorist and criminal identity information;

⁷ DHS report OIG-13-07 "The Visa Waiver Program," November 2012. GAO report GAO-16-498 "Visa Waiver Program," May 2016.

- Several countries⁸ have increased the frequency of their reporting of lost and stolen passports — VWP countries account for over 70 percent of the almost 73 million lost and stolen travel documents reported to INTERPOL;
- Several countries have agreed to adopt new technologies to work with DHS to jointly vet asylum, refugee, and other immigration applications against each other's data, establishing a formidable force multiplier for detecting criminals, terrorists and unqualified applicants; and
- All VWP countries are now issuing and using for travel to the United States fraud-resistant e-passports that meet or exceed the International Civil Aviation Organization standards.

In addition, following the enactment of the VWP Improvement Act, DHS has taken several steps to apply enhanced restrictions on visa-free travel under the VWP for individuals who have traveled to Iran, Iraq, Sudan, Syria, Libya, Somalia, or Yemen or individuals who are dual nationals of Iran, Iraq, Sudan or Syria. Beginning January 13, 2016, CBP initiated a protocol to identify ESTA holders who had travelled to Iraq, Syria, Iran, or Sudan since March 1, 2011 who may be ineligible for future travel if they do not meet the criteria for a waiver allowed for under the Act. On February 18, 2016, DHS announced that individuals who had travelled to Libya, Somalia, and Yemen also may be ineligible for future travel if they do not meet the criteria for a waiver.⁹ Additionally, on January 21, 2016, CBP began denying new ESTA applications and revoking existing ESTAs for individuals who indicated dual nationality with Iran, Iraq, Sudan, or Syria.

In November 2014, in response to increasing concerns regarding foreign terrorist fighters, DHS strengthened the security of the VWP through the addition of new data elements to the ESTA application. These enhancements included a series of additional questions a VWP traveler must answer on the ESTA application, to include other names/aliases, citizenships, contact information, and city of birth.

Arrival Processing

CBP's use of advance information, its pre-departure targeting operations, and its overseas footprint all comprise critical parts of CBP's multi-layered security strategy to address concerns long before they reach the physical border of the United States. U.S. law requires all private and commercial air and sea carriers operating routes to, from, or through the United States to provide API and PNR data to CBP. These data, which include travelers' biographic and travel reservation information, are screened against U.S. and international law enforcement and counterterrorism databases to identify high-risk individuals before they fly to the United States. Even if issued a visa or other travel authorization, however, it is important to note that upon arrival in the United States, all persons are subject to inspection by CBP Officers. CBP Officers review entry documents, query CBP and other law enforcement databases, collect biometrics

⁸ Including Brunei, Greece, Hungary, and Portugal.

⁹In FY 2016, since implementing the new travel and dual nationality restrictions to the Visa Waiver Program, CBP denied, canceled, or revoked 39,303 ESTA applications. These individuals would not be eligible to travel under the VWP.

(including from VWP travelers),¹⁰ and interview all travelers to determine the purpose and intent of their travel, and whether any further inspection is necessary based on, among other things, national security, admissibility, customs, or agriculture concerns.

Of note, CBP's Tactical Terrorism Response Teams (TTRT) are deployed at U.S. POEs and consist of CBP Officers who are specially trained in counterterrorism response. TTRT Officers utilize information derived from targeting and inspection to mitigate possible threats. TTRT officers are immersed in the current and developing threat picture through the continuous review of information, and are responsible for the examination of travelers identified within the Terrorist Screening Database, and other travelers suspected of having a nexus to terrorism who arrive to a POE. For FY 2017 to date¹¹, as a result of the dedicated efforts of the men and women serving on CBP's TTRT, and the information discovered during secondary inspection, nearly 600 people who had been granted visas or other travel documents, or had an approved ESTA, have been refused admission to the United States. CBP Officers and Agents remain our last line of defense against those who would seek to enter the country to do us harm.

In addition, CBP Officers remove from circulation counterfeit, fraudulent, and altered travel documents, as well as lost or stolen travel documents presented for use by an individual other than the rightful holder, such as those presented by impostors. CBP currently uses 1:1 facial comparison technology at select primary lanes at John F. Kennedy International Airport and Washington Dulles International Airport on U.S. and non-U.S. travelers arriving in the United States. This technology enables CBP Officers to use facial recognition technology as a tool to assist in determining whether an individual presenting a valid e-passport is the same individual whose photograph is contained in that passport. In those cases where the CBP Officer is unsure of the traveler's true identity, the traveler is referred for additional checks to confirm identity or to document fraudulent use of a passport. Since this technology was deployed in early 2016, over 400,000 travelers have had their identities confirmed with the use of 1:1 facial comparison technology.

Finally, CBP's Fraudulent Document Analysis Unit (FDAU) serves as the central repository and point of analysis for all fraudulent travel documents interdicted or recovered by CBP personnel. FDAU analysis of fraudulent documents provides intelligence, alerts and training back to the field, as well as serves as a mechanism to remove fraudulent documents from circulation to prevent their further use – a lesson learned from the 9/11 Commission Report. This cyclical process adds a layer of security to the homeland by removing an additional opportunity for misuse.

Identifying and Apprehending Threats to National Security and Public Safety within the United States

An important mission of DHS is to actively identify and initiate enforcement action on persons who have overstayed their terms of admission in the United States and who pose a threat to national security, border security, or public safety. ICE undertakes this very important activity for DHS. Within ICE, there are dedicated units, special agents, analysts, and systems in place to

¹⁰ Biometrics are collected for most foreign nationals arriving at U.S. airports.

¹¹ As of April 19, 2017

address nonimmigrant overstays. Through investigative efforts, ICE analyzes and determines which overstay leads may be suitable for further national security investigation. Once leads are received, ICE conducts both batch and manual vetting against government databases, public indices, and social media (when appropriate). This vetting helps determine if an individual who overstayed has departed the United States, adjusted to a lawful status, has a pending immigration benefit application, or would be appropriate for an enforcement action.

As part of this tiered review, ICE prioritizes nonimmigrant overstay cases through risk-based analysis. ICE Homeland Security Investigation's (HSI) Counterterrorism and Criminal Exploitation Unit (CTCEU) oversees the national program dedicated to the investigation of nonimmigrant visa violators who may pose a national security risk and/or public safety concern. Each year, CTCEU analyzes records of hundreds of thousands of potential status violators after preliminary analysis of data from various government systems, including the Student and Exchange Visitor Information System (SEVIS) and CBP's Arrival and Departure Information System (ADIS), along with other information. After this analysis, CTCEU establishes compliance or departure dates from the United States and/or determines potential violations that warrant field investigations.

CTCEU proactively develops cases for investigation in furtherance of the overstay mission, monitors the latest threat reports, and addresses emergent issues. This practice, which is designed to detect and identify individuals exhibiting specific risk factors based on intelligence reporting, travel patterns, and in-depth criminal research and analysis, has contributed to DHS's counterterrorism mission by initiating and supporting high-priority national security initiatives based on specific intelligence.

In FY 2015, CTCEU reviewed 971,305 leads regarding potential overstays. Numerous leads were closed through an automated screening and vetting process. The most common reason for closure was subsequent departure from the United States. A total of 9,968 leads were sent to HSI field offices for investigation. As a result in FY 2015 alone, HSI made 1,910 arrests, secured 86 indictments, and obtained 80 convictions.

CTCEU refers leads that do not meet ICE HSI criteria for further investigation to ICE Enforcement and Removal Operations' National Criminal Analysis and Targeting Center.

Conclusion

The men and women of DHS and its Component Agencies do a tremendous job every day to protect our country. As terrorists and criminals change their methods and tactics and technologies continue to evolve, DHS will work with its interagency and foreign partners— as well as private sector partners — to adapt and respond swiftly and effectively to prevent their entry into the United States.

Thank you again for the opportunity to testify today. We look forward to answering your questions.



TESTIMONY OF

MICHAEL DOUGHERTY

Acting Assistant Secretary for Border, Immigration, and Trade
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security

JOHN WAGNER

Deputy Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection
Department of Homeland Security

CLARK E. SETTLES

Assistant Director, National Security Investigations
U.S. Immigration and Customs Enforcement
Department of Homeland Security

BEFORE THE

U.S. House of Representatives

Committee on Homeland Security
Taskforce on Denying Terrorist Entry into the United States

ON

Denying Terrorists Entry to the United States: Examining Visa Security

May 3, 2017
Washington, DC

Introduction

Chairman Gallagher, Ranking Member Watson Coleman, and distinguished Committee Members.

Thank you for the opportunity to appear before you today to discuss the efforts of the Department of Homeland Security (DHS) to prevent terrorists and other criminal actors from entering the United States, either by acquiring U.S. visas or traveling through the Visa Waiver Program (VWP). This work involves close interagency collaboration and partnership with foreign governments. Ultimately, traveler screening and vetting is an integral component of our responsibility to protect the homeland, and DHS employs a multi-layered strategy to do so.

Furthermore, as called for in Section 5 of the President's Executive Order (EO) 13780, *Protecting The Nation From Foreign Terrorist Entry Into The United States*, DHS is diligently working with the Departments of State (DOS) and Justice and the Office of the Director of National Intelligence (ODNI) to implement a uniform baseline for screening and vetting standards and procedures. These standards seek "to identify individuals who seek to enter the United States on a fraudulent basis, who support terrorism, violent extremism, acts of violence toward any group or class of people within the United States, or who present a risk of causing harm subsequent to their entry."

DHS Secretary John F. Kelly has made clear that blocking terrorists and criminals from accessing the United States is one of his highest priorities, and the Administration is undertaking serious and sustained efforts to ensure that we keep bad actors from reaching our shores and endangering our people. As part of this effort, we are modernizing screening, expanding information sharing within our government and with foreign partners, and exploring innovative approaches for detecting threat actors. By focusing on better obstructing terrorists and criminals, we can more effectively facilitate legitimate trade and travel.

Pushing Out the Zone of Security

Secretary Kelly noted in his remarks at George Washington University on April 18, 2017, that "[t]he more we push our borders out, the safer our homeland will be." The Secretary went on to highlight in those remarks the importance of knowing who is coming into the country and what their intent for coming is prior to their arrival "at our doorstep." There are a multitude of activities, efforts, and programs that DHS and its Component Agencies undertake to do just that.

In Fiscal Year (FY) 2016, U.S Customs and Border Protection (CBP) inspected over 390 million travelers at 328 ports of entry (POE), of which over 119 million flew into air POEs. CBP's pre-departure strategy is one of the ways by which DHS assists our interagency, foreign government, and private sector partners to deny international travel to potential terrorists and criminals. A major component of this strategy is the recommendation of denial of visas, as well as denial and/or revocation of visa waiver approvals to individuals who may present a risk to national security or public safety. It is a risk-based, intelligence-driven strategy that extends our border security efforts outward to detect, assess, and mitigate, at the earliest possible point in the travel continuum, any risk posed by travelers before they reach the United States. As threats evolve,

CBP works in close partnership with our foreign counterparts – including those in Europe, North Africa, and the Middle East – to develop greater situational awareness of emerging threats, leverage partner capabilities to affect threat networks, and coordinate enforcement actions. These concerns are not limited to the United States and there is a growing international commitment to combating these shared threats to our security.

U.S. Immigration and Customs Enforcement (ICE) also actively works to push our defenses outward. To achieve this goal, ICE forward deploys personnel to 66 offices in 49 countries. ICE’s international staff works in conjunction with overseas law enforcement counterparts to detect, disrupt, and dismantle transnational criminal groups and individuals who seek to harm our country and people. Furthermore, ICE special agents investigate transnational crime by conducting a wide range of criminal investigations in coordination with our foreign and domestic partner agencies, targeting the illegal movement of people, merchandise and monetary instruments into, within, and out of the United States.

Visa and Travel Authorization Security

As President Trump has stated, “Homeland Security is in the business of saving lives, and that mandate will guide our actions.” Since taking office this Administration has worked tirelessly to enhance border security, promote public safety, and minimize the threat of terrorist attacks by foreign nationals in the United States. Part of this process is ensuring the security of international travel by preventing dangerous persons from obtaining visas, travel authorizations, and boarding passes. Before boarding a flight or vessel destined for the United States, most foreign nationals must obtain a non-immigrant visa from the DOS — issued at a U.S. Embassy or Consulate. The visa process involves multiple security checks, including screening of applicants against a wide array of criminal and terrorist databases to verify the individual’s identity and to detect derogatory information that might lead to an inadmissibility determination, as well as an in-person interview with the applicant.

CBP also conducts vetting of all valid immigrant and non-immigrant visas. Although the visa application and adjudication processes rest with the DOS, CBP’s National Targeting Center (NTC) conducts continuous vetting of U.S. immigrant and nonimmigrant visas that have been recently issued or revoked. Recurrent vetting ensures that changes in a traveler’s admissibility and eligibility for travel are identified in near real-time, allowing CBP to immediately determine if it is necessary to take action prior to subject’s arrival to the United States, such as a “no board” recommendation to a carrier, and/or a recommendation to the DOS to revoke the visa.

In an effort to augment and expand visa security operations, ICE manages the Visa Security Program (VSP) for DHS. VSP’s primary purpose is to identify terrorists, criminals, and other individuals who pose a threat or are otherwise ineligible for visas prior to visa adjudication or application for admission to the United States. VSP operations are currently conducted at 30 visa-issuing posts in 25 countries.

Through the VSP, ICE deploys special agents to visa issuing posts worldwide to utilize available investigative resources, in-person interviews, and collaboration between U.S. agencies and our foreign counterparts, in order to investigate and disrupt the travel of suspect individuals during

the visa application process. Experience has shown the Department that there is no technological substitute for having experienced ICE special agents deployed overseas to apply law enforcement capabilities to the visa process through investigative measures, informed interviews with suspect applicants, and leveraging local contacts for information.

Special Agents assigned to international VSP posts are supported through domestic-based screening and vetting of visa applicants, the Pre-Adjudicated Threat Recognition and Intelligence Operations Team (PATRIOT). PATRIOT is an interagency endeavor between ICE and CBP's NTC. Through PATRIOT, VSP conducts automated screening of visa application information against DHS holdings, as well as holdings of other U.S. agencies, prior to the visa applicant's interview and visa adjudication. Derogatory information discovered during automated screening is manually vetted and analyzed by domestic PATRIOT personnel using law enforcement, open source, and classified information. PATRIOT analysts then provide deployed VSP personnel with relevant information prior to interviews and other investigative activities. Following an analysis of all known derogatory information, deployed ICE special agents provide a unified DHS recommendation on visa eligibility to DOS consular officers.

In FY 2016, VSP deployed special agents and PATRIOT personnel facilitated the screening and vetting of more than 2.2 million visa applicants, recommended the refusal of more than 8,500 visas, and submitted 1,669 Terrorist Screening Center Database nominations. The VSP will expand to two additional posts in FY 2017 and is tentatively scheduled to add an additional two posts in FY 2018.

If travelers are eligible to travel under the VWP, they must apply for and be approved for a travel authorization via the Electronic System for Travel Authorization (ESTA). Through ESTA, CBP conducts enhanced vetting of potential VWP travelers to assess whether they are eligible to travel under the VWP or could pose a risk to the United States or the public at large. All ESTA applications are screened against security and law enforcement databases, and CBP automatically refuses authorization to individuals who are found to be ineligible to travel to the United States under the VWP. Similarly, current and valid ESTAs may be revoked if concerns arise through recurrent vetting.¹

In November 2016, CBP launched the Electronic Visa Update System (EVUS). Similar to ESTA, EVUS is an online system used by visa holders to periodically update their biographic information to facilitate their travel to the United States.² To maintain a valid visa for purposes of seeking admission to the United States, travelers with designated nonimmigrant visas from identified countries are required to maintain a valid EVUS enrollment before travelling to the United States. Enrollments generally last for two years or when the traveler's visa or passport expires, whichever comes first. Data collected through EVUS helps us determine whether such travel poses a law enforcement or security risk by checking against select law enforcement

¹ Recurrent vetting is ongoing throughout the period of validity of the ESTA. ESTA applicants who are denied may apply for a nonimmigrant visa.

² At this time, EVUS is only a requirement for individuals travelling on passports issued by the People's Republic of China who have been issued unrestricted, maximum validity B-1 (visitor for business) or B-2 (visitor for pleasure) visas, generally valid for 10 years, Chinese nationals. The requirement is new, and the U.S. Government expects that it may be applied to additional countries or nonimmigrant categories may be designated in the future.

databases and queries law enforcement databases that include terrorist screening, lost/stolen passports, INTERPOL wants/warrants, and immigration violations.

Finally, thanks to the support of Congress, the *Department of Homeland Security Appropriations Act of 2015*³ provided the necessary funds for CBP to initiate counter-network operations within the NTC. The newly-established Counter Network Division's (CND) mission supports CBP, other DHS Components, and interagency law enforcement and Intelligence Community partners to develop an interoperable counter-network process that provides a comprehensive understanding of emerging threats, including those emanating from terrorism, special interest aliens, transnational organized crime and illicit trade networks. Informed through identification of the tactics, techniques, and procedures of adversarial networks – including their efforts to exploit legitimate travel pathways and processes such as the visa process and the VWP – the CND quickly develops analytic solutions and makes those available across DHS components to mitigate further risk.

Visa Waiver Program

An important way in which DHS is pushing out the zone of security is to work with our international partners, including those countries who are members of the VWP. DHS's focus and priority for the VWP is to make it a comprehensive security partnership with America's closest allies. The VWP must be a security program first and foremost—merging together best practices in national security, law enforcement security, and immigration security; and providing the United States with an effective tool for fostering and deepening our national security relationships with key partner countries. As Secretary Kelly recently indicated, we have to continue to look at ways to strengthen the security of the VWP given the threat of foreign fighters returning from the battlefields of Syria and Iraq. DHS is committed to fully ensuring that the VWP is serving the security interests of the United States.

Currently, 38 countries^{4,5} participate in the VWP, which allows their nationals to travel to the United States for business or tourism for stays of up to 90 days (with certain exceptions) after applying and being approved through the ESTA.⁶ In return, these countries must prove that measurable and consistently high requirements are met, including: that information sharing practices enable the rapid relay of information concerning known and suspected terrorists and serious criminals; that lost and stolen passport information is consistently and timely reported; that robust border and travel document security practices are in place; and that effective traveler and migrant screening practices are standard operations. VWP countries also undergo regular,

³ Pub.L. No. 114-4.

⁴ VWP-eligible countries: Andorra, Australia, Austria, Belgium, Brunei, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, The Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, Taiwan, United Kingdom.

⁵ Per the Taiwan Relations Act of 1979, all references to “country” or “countries” in this document also apply with respect to Taiwan.

⁶ Exceptions include citizens of countries under other visa exempt authority, such as Canada. Citizens of countries under visa exempt authority traveling to entering the United States via air are subjected to CBP's vetting and inspection processes prior to their departure for the United States. In the land environment, they are subject to CBP processing upon arrival at a U.S. port of entry.

in-depth security assessments conducted by DHS in consultation with DOS to ensure compliance with these requirements.

The assessments of a VWP country's security standards and operations are among the broadest and most consequential reviews conducted under any U.S. Government program. Rigorous national-level assessments are used to ensure that countries meet the security standards required for continued participation in the Program. DHS, in coordination with the DOS and the Intelligence Community, conducts statutorily-required reviews of each VWP country at least once every two years. The VWP assessment evaluates the country's counterterrorism and law enforcement capabilities, immigration enforcement policies and procedures, passport production and issuance processes, and border security traveler screening capabilities. As needed, the review may also include a site visit where an integrated U.S. Government team conducts thorough inspections of airports, seaports, land borders, and passport production and issuance facilities in the VWP country and holds discussions with the host government, counterterrorism, intelligence, law enforcement, border security, and immigration officials. DHS submits a Report to Congress upon the completion of the assessment. Notably, both the Government Accountability Office (GAO) and the DHS Office of the Inspector General (OIG) have reviewed and written favorably of the methodology DHS uses in conducting these assessments.⁷

Separately, DHS also conducts an annual assessment of all 38 VWP countries against the risk criteria defined in the *Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015* (VWP Improvement Act), passed under this Committee's leadership, and engages in ongoing monitoring of member countries to rapidly identify emerging threats and vulnerabilities.

The bottom line is that in order to join or continue in the VWP, a country cannot represent a threat to the United States and must be working as a partner to prevent terrorist travel. In all instances, the Secretary of Homeland Security retains the statutory authority to suspend or terminate a country's participation in the VWP if there is a credible threat originating from that country that poses an imminent danger to the United States or its citizens.

Under the VWP Improvement Act, VWP countries are now required to issue high-security electronic passports (e-passports); implement information sharing arrangements to exchange criminal and terrorist identity information; establish mechanisms to validate e-passports at each key POE; report all lost and stolen passports to INTERPOL or directly to the United States no later than 24 hours after the country becomes aware of the loss or theft; conclude a U.S. Federal Air Marshals agreement; collect and analyze Advance Passenger Information (API)/Passenger Name Record (PNR) information to identify high-risk travelers; screen international travelers against the INTERPOL Stolen and Lost Travel Documents (SLTD) database and notices; report foreign fighters to multilateral security organizations, such as INTERPOL or EUROPOL; and cooperate with the United States in the screening of refugees and asylum seekers.

Since passage of the Act, DHS has confirmed the following changes among VWP countries:

- An increase in the sharing of terrorist and criminal identity information;

⁷ DHS report OIG-13-07 "The Visa Waiver Program," November 2012. GAO report GAO-16-498 "Visa Waiver Program," May 2016.

- Several countries⁸ have increased the frequency of their reporting of lost and stolen passports — VWP countries account for over 70 percent of the almost 73 million lost and stolen travel documents reported to INTERPOL;
- Several countries have agreed to adopt new technologies to work with DHS to jointly vet asylum, refugee, and other immigration applications against each other's data, establishing a formidable force multiplier for detecting criminals, terrorists and unqualified applicants; and
- All VWP countries are now issuing and using for travel to the United States fraud-resistant e-passports that meet or exceed the International Civil Aviation Organization standards.

In addition, following the enactment of the VWP Improvement Act, DHS has taken several steps to apply enhanced restrictions on visa-free travel under the VWP for individuals who have traveled to Iran, Iraq, Sudan, Syria, Libya, Somalia, or Yemen or individuals who are dual nationals of Iran, Iraq, Sudan or Syria. Beginning January 13, 2016, CBP initiated a protocol to identify ESTA holders who had travelled to Iraq, Syria, Iran, or Sudan since March 1, 2011 who may be ineligible for future travel if they do not meet the criteria for a waiver allowed for under the Act. On February 18, 2016, DHS announced that individuals who had travelled to Libya, Somalia, and Yemen also may be ineligible for future travel if they do not meet the criteria for a waiver.⁹ Additionally, on January 21, 2016, CBP began denying new ESTA applications and revoking existing ESTAs for individuals who indicated dual nationality with Iran, Iraq, Sudan, or Syria.

In November 2014, in response to increasing concerns regarding foreign terrorist fighters, DHS strengthened the security of the VWP through the addition of new data elements to the ESTA application. These enhancements included a series of additional questions a VWP traveler must answer on the ESTA application, to include other names/aliases, citizenships, contact information, and city of birth.

Arrival Processing

CBP's use of advance information, its pre-departure targeting operations, and its overseas footprint all comprise critical parts of CBP's multi-layered security strategy to address concerns long before they reach the physical border of the United States. U.S. law requires all private and commercial air and sea carriers operating routes to, from, or through the United States to provide API and PNR data to CBP. These data, which include travelers' biographic and travel reservation information, are screened against U.S. and international law enforcement and counterterrorism databases to identify high-risk individuals before they fly to the United States. Even if issued a visa or other travel authorization, however, it is important to note that upon arrival in the United States, all persons are subject to inspection by CBP Officers. CBP Officers review entry documents, query CBP and other law enforcement databases, collect biometrics

⁸ Including Brunei, Greece, Hungary, and Portugal.

⁹In FY 2016, since implementing the new travel and dual nationality restrictions to the Visa Waiver Program, CBP denied, canceled, or revoked 39,303 ESTA applications. These individuals would not be eligible to travel under the VWP.

(including from VWP travelers),¹⁰ and interview all travelers to determine the purpose and intent of their travel, and whether any further inspection is necessary based on, among other things, national security, admissibility, customs, or agriculture concerns.

Of note, CBP's Tactical Terrorism Response Teams (TTRT) are deployed at U.S. POEs and consist of CBP Officers who are specially trained in counterterrorism response. TTRT Officers utilize information derived from targeting and inspection to mitigate possible threats. TTRT officers are immersed in the current and developing threat picture through the continuous review of information, and are responsible for the examination of travelers identified within the Terrorist Screening Database, and other travelers suspected of having a nexus to terrorism who arrive to a POE. For FY 2017 to date¹¹, as a result of the dedicated efforts of the men and women serving on CBP's TTRT, and the information discovered during secondary inspection, nearly 600 people who had been granted visas or other travel documents, or had an approved ESTA, have been refused admission to the United States. CBP Officers and Agents remain our last line of defense against those who would seek to enter the country to do us harm.

In addition, CBP Officers remove from circulation counterfeit, fraudulent, and altered travel documents, as well as lost or stolen travel documents presented for use by an individual other than the rightful holder, such as those presented by impostors. CBP currently uses 1:1 facial comparison technology at select primary lanes at John F. Kennedy International Airport and Washington Dulles International Airport on U.S. and non-U.S. travelers arriving in the United States. This technology enables CBP Officers to use facial recognition technology as a tool to assist in determining whether an individual presenting a valid e-passport is the same individual whose photograph is contained in that passport. In those cases where the CBP Officer is unsure of the traveler's true identity, the traveler is referred for additional checks to confirm identity or to document fraudulent use of a passport. Since this technology was deployed in early 2016, over 400,000 travelers have had their identities confirmed with the use of 1:1 facial comparison technology.

Finally, CBP's Fraudulent Document Analysis Unit (FDAU) serves as the central repository and point of analysis for all fraudulent travel documents interdicted or recovered by CBP personnel. FDAU analysis of fraudulent documents provides intelligence, alerts and training back to the field, as well as serves as a mechanism to remove fraudulent documents from circulation to prevent their further use – a lesson learned from the 9/11 Commission Report. This cyclical process adds a layer of security to the homeland by removing an additional opportunity for misuse.

Identifying and Apprehending Threats to National Security and Public Safety within the United States

An important mission of DHS is to actively identify and initiate enforcement action on persons who have overstayed their terms of admission in the United States and who pose a threat to national security, border security, or public safety. ICE undertakes this very important activity for DHS. Within ICE, there are dedicated units, special agents, analysts, and systems in place to

¹⁰ Biometrics are collected for most foreign nationals arriving at U.S. airports.

¹¹ As of April 19, 2017

address nonimmigrant overstays. Through investigative efforts, ICE analyzes and determines which overstay leads may be suitable for further national security investigation. Once leads are received, ICE conducts both batch and manual vetting against government databases, public indices, and social media (when appropriate). This vetting helps determine if an individual who overstayed has departed the United States, adjusted to a lawful status, has a pending immigration benefit application, or would be appropriate for an enforcement action.

As part of this tiered review, ICE prioritizes nonimmigrant overstay cases through risk-based analysis. ICE Homeland Security Investigation's (HSI) Counterterrorism and Criminal Exploitation Unit (CTCEU) oversees the national program dedicated to the investigation of nonimmigrant visa violators who may pose a national security risk and/or public safety concern. Each year, CTCEU analyzes records of hundreds of thousands of potential status violators after preliminary analysis of data from various government systems, including the Student and Exchange Visitor Information System (SEVIS) and CBP's Arrival and Departure Information System (ADIS), along with other information. After this analysis, CTCEU establishes compliance or departure dates from the United States and/or determines potential violations that warrant field investigations.

CTCEU proactively develops cases for investigation in furtherance of the overstay mission, monitors the latest threat reports, and addresses emergent issues. This practice, which is designed to detect and identify individuals exhibiting specific risk factors based on intelligence reporting, travel patterns, and in-depth criminal research and analysis, has contributed to DHS's counterterrorism mission by initiating and supporting high-priority national security initiatives based on specific intelligence.

In FY 2015, CTCEU reviewed 971,305 leads regarding potential overstays. Numerous leads were closed through an automated screening and vetting process. The most common reason for closure was subsequent departure from the United States. A total of 9,968 leads were sent to HSI field offices for investigation. As a result in FY 2015 alone, HSI made 1,910 arrests, secured 86 indictments, and obtained 80 convictions.

CTCEU refers leads that do not meet ICE HSI criteria for further investigation to ICE Enforcement and Removal Operations' National Criminal Analysis and Targeting Center.

Conclusion

The men and women of DHS and its Component Agencies do a tremendous job every day to protect our country. As terrorists and criminals change their methods and tactics and technologies continue to evolve, DHS will work with its interagency and foreign partners— as well as private sector partners — to adapt and respond swiftly and effectively to prevent their entry into the United States.

Thank you again for the opportunity to testify today. We look forward to answering your questions.



Testimony

Before the Task Force on Denying
Terrorists Entry into the United States,
Committee on Homeland Security,
House of Representatives

For Release on Delivery
Expected at 2 p.m. ET
Wednesday, May 3, 2017

BORDER SECURITY

Progress and Challenges in DHS's Efforts to Address High-Risk Travelers and Strengthen Visa Security

Statement of Rebecca Gambler, Director,
Homeland Security and Justice

GAO Highlights

Highlights of [GAO-17-599T](#), a testimony before the Task Force on Denying Terrorists Entry into the United States, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

DHS seeks to identify and interdict travelers who are potential security threats to the United States, such as foreign fighters and potential terrorists, human traffickers, drug smugglers and otherwise inadmissible persons, at the earliest possible point in time. DHS also adjudicates petitions for certain visa categories and has certain responsibilities for strengthening the security of the visa process, including oversight of VSP and VWP. State manages the visa adjudication process for foreign nationals seeking admission to the United States.

This statement addresses (1) CBP programs aimed at preventing high-risk travelers from boarding U.S.-bound flights; (2) ICE's management of VSP; and (3) DHS's oversight of VWP. This statement is based on prior products GAO issued from March 2011 through January 2017, along with selected updates conducted in April 2017 to obtain information from DHS on actions it has taken to address prior GAO recommendations.

What GAO Recommends

GAO previously made recommendations to improve evaluation of CBP's predeparture programs' performance and strengthen DHS's oversight of VSP and VWP. DHS agreed with GAO's recommendations related to CBP's predeparture programs and VWP. DHS did not agree with some of GAO's recommendations related to VSP. GAO has ongoing work related to, among other things, DHS's management and oversight of VSP and plans to report later this year on the results of this work.

View [GAO-17-599T](#). For more information, contact Rebecca Gambler at (202) 512-8777 or gambler@gao.gov.

May 3, 2017

BORDER SECURITY

Progress and Challenges in DHS's Efforts to Address High-Risk Travelers and Strengthen Visa Security

What GAO Found

In January 2017, GAO reported that the Department of Homeland Security's (DHS) U.S. Customs and Border Protection (CBP) operates predeparture programs to help identify and interdict high-risk travelers before they board U.S.-bound flights. CBP officers inspect all U.S.-bound travelers on precleared flights at the 15 Preclearance locations and, if deemed inadmissible, a traveler will not be permitted to board the aircraft. CBP also operates nine Immigration Advisory Program and two Joint Security Program locations, as well as three Regional Carrier Liaison Groups, through which CBP may recommend that air carriers not permit identified high-risk travelers to board U.S.-bound flights. CBP data showed that it identified and interdicted over 22,000 high-risk air travelers through these programs in fiscal year 2015 (the most recent data available at the time of GAO's report). However, CBP had not fully evaluated the overall effectiveness of these programs using performance measures and baselines. CBP tracked some data, such as the number of travelers deemed inadmissible, but had not set baselines to determine if predeparture programs are achieving goals, consistent with best practices for performance measurement. GAO recommended that CBP develop and implement a system of performance measures and baselines to better position CBP to assess if the programs are achieving their goals. CBP concurred and has established a working group to develop such measures and baselines.

In March 2011, GAO reported on the Visa Security Program (VSP) through which DHS's U.S. Immigration and Customs Enforcement (ICE) deploys personnel to certain U.S. overseas posts to review visa applications. Among other things, GAO found that ICE did not collect comprehensive data on all VSP performance measures or track the time officials spent on visa security activities. DHS did not concur with GAO's recommendations to address these limitations, stating that ICE collected data on all the required performance measures and tracked VSP case investigation hours. However, GAO continues to believe DHS needs to address these limitations. GAO has ongoing work assessing U.S. agencies' efforts to strengthen the security of the visa process, including oversight of VSP, in which GAO plans to follow up on the findings and recommendations from its March 2011 report related to ICE's efforts to enhance VSP performance measurement.

In May 2016, GAO reported on DHS's oversight of the Visa Waiver Program (VWP), which allows nationals from 38 countries to travel visa-free to the United States for business or pleasure for 90 days or less. GAO reported, among other things, that all 38 countries entered into required agreements, or their equivalents, to (1) report lost and stolen passports, (2) share identity information about known or suspected terrorists, and (3) share criminal history information. However, not all countries shared such information. In August 2015, DHS established a new requirement for VWP countries to implement the latter two agreements; however, DHS did not establish time frames for instituting the amended requirements. GAO recommended that DHS work with VWP countries to implement these agreements and DHS concurred. As of April 2017, DHS reported that officials are continuing to work with VWP countries on time frames for implementing program requirements.

May 3, 2017

Chairman Gallagher, Ranking Member Watson Coleman, and Members of the Task Force:

I am pleased to be here today to discuss GAO's body of work on U.S. government programs and activities related to screening foreign nationals seeking to travel to the United States on a temporary basis—either with a nonimmigrant visa, or in some cases, without a visa.¹ Each year, millions of such temporary visitors legally enter the United States. From fiscal year 2010 through fiscal year 2015, the Department of State (State) issued more than 52 million visas for business travel, pleasure, or for foreign and cultural exchange student programs, among other things. In addition, from fiscal year 2010 through fiscal year 2015, more than 116 million visitors were admitted to the United States under the Visa Waiver Program (VWP), which allows nationals from 38 countries to apply for admission to the country as temporary visitors for business or pleasure without first obtaining a visa from a U.S. embassy or consulate abroad.²

The Department of Homeland Security (DHS) seeks to identify and interdict travelers who are potential security threats to the United States, such as foreign fighters and potential terrorists, human traffickers, drug smugglers, and otherwise inadmissible persons, at the earliest possible

¹Throughout this statement we generally use the term “foreign national” to refer to an “alien,” which is defined under U.S. immigration law as any person who is not a U.S. citizen or national. See 8 U.S.C. § 1101(a)(3). In addition, temporary visitors are foreign nationals present in the United States on a temporary basis pursuant to a specific nonimmigrant category (see 8 U.S.C. § 1101(a)(15); see also 8 C.F.R. § 214.1(a)(1)-(2)), including those who are allowed to seek admission without a visa, such as Mexican nationals and citizens of Canada and the British Overseas Territory of Bermuda (and certain residents of other adjacent islands, such as the Bahamas) under certain circumstances, as well as Visa Waiver Program (VWP) participants. See 8 C.F.R. §§ 212.1, 214.6(d); 22 C.F.R. §§ 41.0 to 41.3. Foreign nationals seeking permanent status in the United States must generally obtain an immigrant visa, which provides a path to lawful permanent residency. For the purposes of this statement, we use the term “visa” in reference to a nonimmigrant visa.

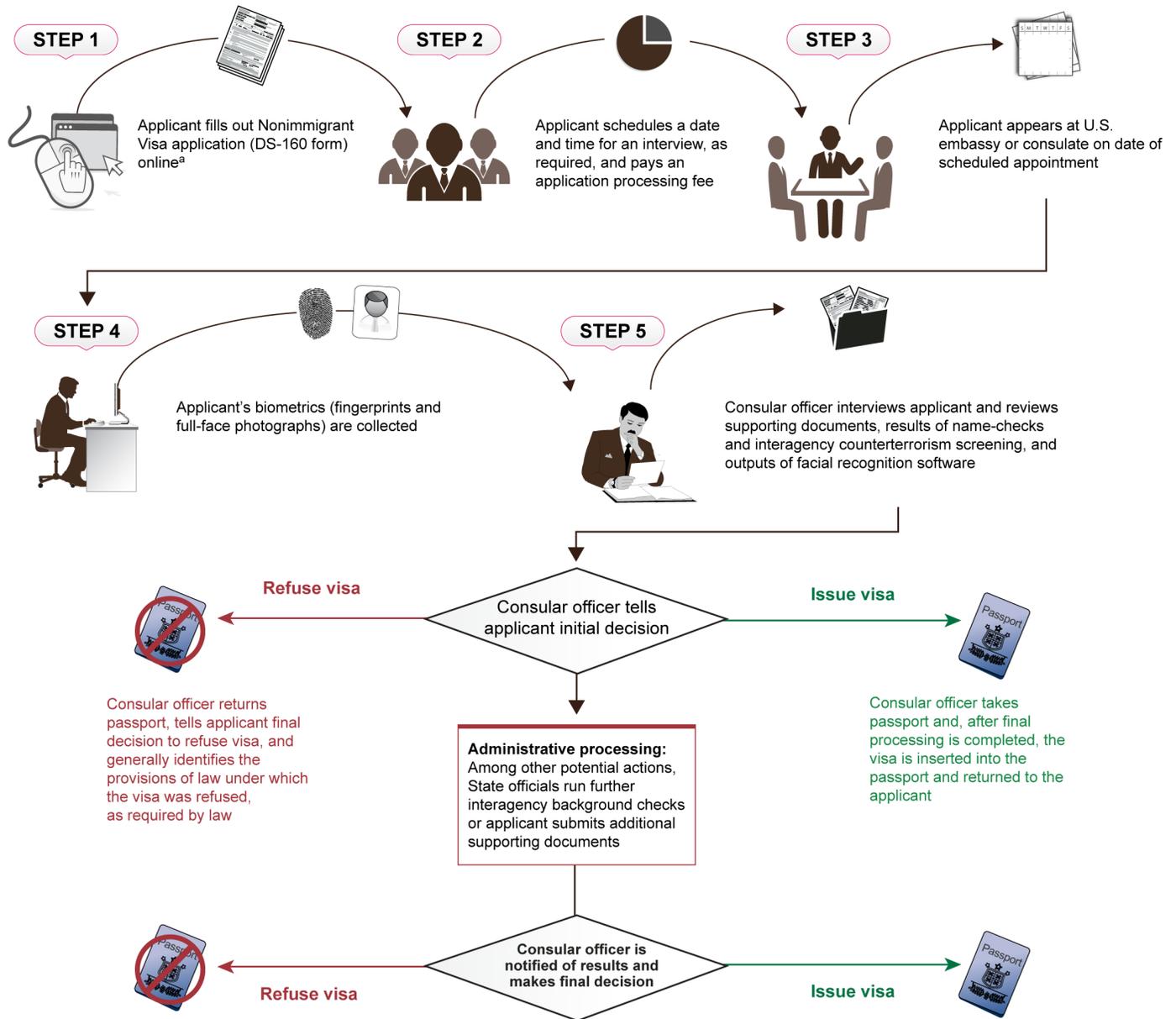
²See 8 U.S.C. § 1187. The VWP was established in 1986 as a pilot program, under which the nationals of up to eight designated countries which extended reciprocal privileges to U.S. citizens and nationals and fulfilled certain other program criteria, would not need a visa for admission to the United States as temporary visitors during the pilot program period. See Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, tit. III, pt. B, § 313, 100 Stat. 3359, 3435-39. VWP became a permanent program in October 2000. See Visa Waiver Permanent Program Act, Pub. L. No. 106-396, tit. I, § 101, 114 Stat. 1637 (2000).

point in the travel lifecycle to make the nation's physical borders the last, not the first, line of defense.³ DHS adjudicates petitions for certain visa categories, and also has certain responsibilities for strengthening the security of the visa process, including establishing visa policy and managing the VWP. In particular, DHS's U.S. Customs and Border Protection (CBP) is tasked with, among other duties, securing U.S. borders and processing all travelers on U.S.-bound flights; inspecting all people entering or applying for admission to the United States; and screening VWP applicants to determine their eligibility to travel to the United States under the program. In addition, DHS's U.S. Immigration and Customs Enforcement (ICE) oversees the Visa Security Program (VSP) under which it deploys officials to certain U.S. embassies and consulates to strengthen the visa process by working with State officials in reviewing visa applications. State is responsible for visa adjudication and issuance for foreign nationals seeking admission to the United States and is responsible for managing the consular officer corps and its functions at over 220 visa-issuing posts overseas.

Foreign nationals who wish to come to the United States on a temporary basis and are not citizens or nationals of countries that participate in the VWP must generally obtain a visa authorizing their travel. U.S. law provides for the temporary admission of various categories of nonimmigrants, such as tourists, foreign students, diplomats, and temporary workers, who are admitted for an authorized period of stay, consistent with any time limitation and other terms of admission. The process for determining who will be issued or refused a visa contains several steps, including document reviews; collection of biometrics (fingerprints and full-face photographs); cross-referencing an applicant's name and biometrics against multiple databases maintained by the U.S. government; and in-person interviews. Personal interviews with consular officers are required by law for most foreign nationals seeking visas. For an overview of the visa process, see figure 1.

³Foreign fighters are individuals who leave home, travel abroad to terrorist safe havens, and join or assist violent extremist groups.

Figure 1: Nonimmigrant Visa Application and Adjudication Process



Sources: GAO (analysis); Department of State (data); Art Explosion (clipart). | GAO-17-599T

^aPrior to this step, some nonimmigrant visas require petitioners to file a petition on behalf of the beneficiary, or on their own behalf, as appropriate, with the Department of Homeland Security (DHS). DHS is responsible for approving or denying the petition, notifying the petitioner, and sending the approved petition to the Department of State.

The VWP was established in 1986 to facilitate the legitimate travel of visitors for business or pleasure to the United States. Qualifying nationals from the 38 countries participating in the VWP—for example, France, Germany, and Hungary—may travel without a visa to the United States for business or pleasure stays of up to 90 days.⁴ In 2007, Congress passed the Implementing Recommendations of the 9/11 Commission Act of 2007, which mandated several changes to modernize the program through enhanced bilateral cooperation on critical counterterrorism and information-sharing initiatives, support and expansion of tourism and business opportunities to enhance long-term competitiveness, and strengthening of bilateral relationships.⁵ In particular, the U.S. government began requiring each VWP country to enter into a

- Lost and Stolen Passport (LASP) agreement to report information about the theft or loss of passports,
- Homeland Security Presidential Directive 6 (HSPD-6) arrangement to share watch list information about known or suspected terrorists,⁶ and
- Preventing and Combating Serious Crime (PCSC) agreement to establish frameworks for enhanced law enforcement cooperation, including sharing of criminal history information.

The Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015, which became law in December of that year, amended

⁴The 38 VWP countries include Taiwan. Although the United States does not have diplomatic relations with Taiwan, the Taiwan Relations Act provides that “[w]henever the laws of the United States refer or relate to foreign countries, nations, states, governments, or similar entities, such terms shall include and such laws shall apply with respect to Taiwan.” Pub. L. No. 96-8, § 4(b), 93 Stat. 14, 15 (1979) (classified at 22 U.S.C. § 3303).

⁵Pub. L. No. 110-53, tit. VII, subtit. B, § 711, 121 Stat. 266, 338-45.

⁶Among other things, Homeland Security Presidential Directive/HSPD-6—*Integration and Use of Screening Information*, issued on September 16, 2003, directed the Secretary of State to develop a proposal for enhancing cooperation with certain foreign governments, beginning with those countries for which the U.S. has waived visa requirements, to establish appropriate access to terrorism screening information of the participating governments.

certain requirements to provide enhanced security measures for the program, among other purposes.⁷

My testimony discusses: (1) CBP programs aimed at preventing high-risk travelers from boarding U.S.-bound flights, (2) ICE's management of the VSP, and (3) DHS's oversight of the VWP. This testimony is based on our prior reports, in particular, those published in March 2011, May 2016, and January 2017.⁸ For these reports, we examined program documentation, such as standard operating procedures and agencies' policies and guidance, as well as agency data on program performance. We also interviewed DHS and State officials, among others, in headquarters and at U.S. embassies and consulates. Additional details on the scope and methodology are available in our published reports. In addition, this statement contains updates to selected information from these reports. For the updates, we collected information from DHS on actions it has taken to address findings and recommendations made in prior reports on which this statement is based. All of our work was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

⁷Pub. L. No. 114-113, Div. O, tit. II, 129 Stat. 2242, 2988-95. The law now prohibits individuals who are nationals of VWP countries who have been present in Iran, Iraq, Syria, Sudan, Libya, Somalia or Yemen on or after March 1, 2011, from traveling or being admitted to the United States through the VWP, with certain exceptions. According to CBP, these new eligibility requirements do not bar travel to the United States; instead, a national of a VWP country who does not meet the requirements must obtain a visa for travel to the United States. The law also now requires that countries fully implement passenger information exchange agreements in order to participate in the VWP. Additional requirements have been added regarding machine-readable, electronic passports for individuals; country certifications of a mechanism to validate passports; termination of designation for countries that fail to share information or fail to screen individuals admitted to, or departing, the country for unlawful activity; designation of high-risk program countries that may be suspended from the program; and other enhancements to the electronic system for travel authorization.

⁸GAO, *Border Security: CPB Aims to Prevent High-Risk Travelers from Boarding U.S.-Bound Flights, but Needs to Evaluate Program Performance*, [GAO-17-216](#) (Washington, D.C.: Jan. 24, 2017); *Visa Waiver Program: DHS Should Take Steps to Ensure Timeliness of Information Needed to Protect U.S. National Security*, [GAO-16-498](#) (Washington, D.C.: May 5, 2016); and, *Border Security: DHS's Visa Security Program Needs to Improve Performance Evaluation and Better Address Visa Risk Worldwide*, [GAO-11-315](#) (Washington, D.C.: Mar. 31, 2011).

CBP's Air Predeparture Programs Interdict High-Risk Air Travelers, but CBP Has Not Fully Assessed the Programs' Performance

CBP Identifies and Interdicts High-Risk Travelers before They Board U.S-Bound Flights

As we reported in January 2017, CBP electronically vets all travelers before they board U.S.-bound flights and continues to do so until they land at a U.S. port of entry.⁹ Through these vetting efforts, CBP seeks to identify high-risk travelers from the millions of individuals who travel to the United States each year. As we reported in January 2017, CBP's vetting and targeting efforts are primarily conducted by its National Targeting Center (NTC) and entail (1) traveler data matching and analysis, (2) rules-based targeting, and (3) recurrent vetting. Specifically:

- CBP's primary method of identifying high-risk individuals is through the comparison of travelers' information (such as name, date of birth, and gender)¹⁰ against records extracted from U.S. government databases, including the Terrorist Screening Database (TSDB)—the

⁹GAO-17-216. Ports of entry are facilities that provide for the controlled entry into or departure from the United States. Specifically, a port of entry is any officially designated location (seaport, airport, or land border location) where DHS officers inspect persons entering or applying for admission into, or departing the United States pursuant to U.S. immigration law.

¹⁰According to CBP officials, information from both the Advance Passenger Information System, which includes biographical information such as full name, date of birth, gender, flight number, date of arrival and departure, citizenship, and passport/alien registration card number, among others, and the Passenger Name Record, which refers to reservation information contained in an air carrier's electronic reservation system and/or departure control system that sets forth the identity and travel plans of each traveler or group of travelers included under the same reservation record, are utilized in the targeting and vetting of individuals attempting to travel to the United States. See 49 U.S.C. § 44909; 19 C.F.R. §§ 122.49a, 122.49d.

U.S. government's consolidated terrorist watch list.¹¹ Traveler data matching focuses on identifying known high-risk individuals—that is, individuals who may be inadmissible to the United States under U.S. immigration law or who may otherwise pose a threat to homeland or national security. CBP's primary tool for vetting and targeting travelers is the Automated Targeting System (ATS), which is a computer-based enforcement and support system that compares traveler information against intelligence and law enforcement data to identify high-risk travelers. Traveler data matching occurs throughout the travel process and, upon a positive or possible match, CBP officers can select these individuals for further vetting, interviewing, and inspection.

- CBP's rules-based targeting efforts seek to identify unknown high-risk travelers—that is, travelers for whom U.S. government entities do not have available derogatory information directly linking them to terrorist activities or any other actions that would make them potentially inadmissible to the United States but who may present a threat and thus warrant additional scrutiny. CBP identifies unknown high-risk individuals by comparing their information against a set of targeting rules based on intelligence, law enforcement, and other information. NTC officials stated that these rules have identified potential high-risk travelers, including potential foreign fighters. Rules-based targeting evaluates travelers during the travel process and, in some cases, in advance of the travel process. If a traveler is a rule "hit," this individual can be selected for further vetting, interviewing, and inspection.¹²
- CBP supports its traveler data matching and rules-based targeting efforts through the use of recurrent vetting. NTC's vetting, targeting, and traveler data matching activities in ATS run 24 hours a day and seven days a week and automatically scan updated traveler information, when available. This process is to ensure that new information that affects a traveler's admissibility is identified in near real time. Recurrent vetting occurs throughout the travel process and continues until a traveler arrives at a domestic port of entry. For

¹¹Information in the TSDB comes from two sources: the National Counterterrorism Center, which provides information on known or suspected international terrorists, and the Federal Bureau of Investigation, which provides information about known or suspected domestic terrorists. For more information about the process by which the U.S. government manages this watchlist, see GAO, *Terrorist Watchlist: Routinely Assessing Impacts of Agency Actions since the December 29, 2009, Attempted Attack Could Help Inform Future Efforts*, [GAO-12-476](#) (Washington, D.C.: May 31, 2012).

¹²In general, when a traveler is identified through rules-based targeting, the traveler is considered to have hit a rule.

example, after checking into a foreign airport, a traveler may have his or her visa revoked for a security or immigration-related violation. Due to recurrent vetting, CBP would be alerted to this through ATS and could take action, as appropriate.

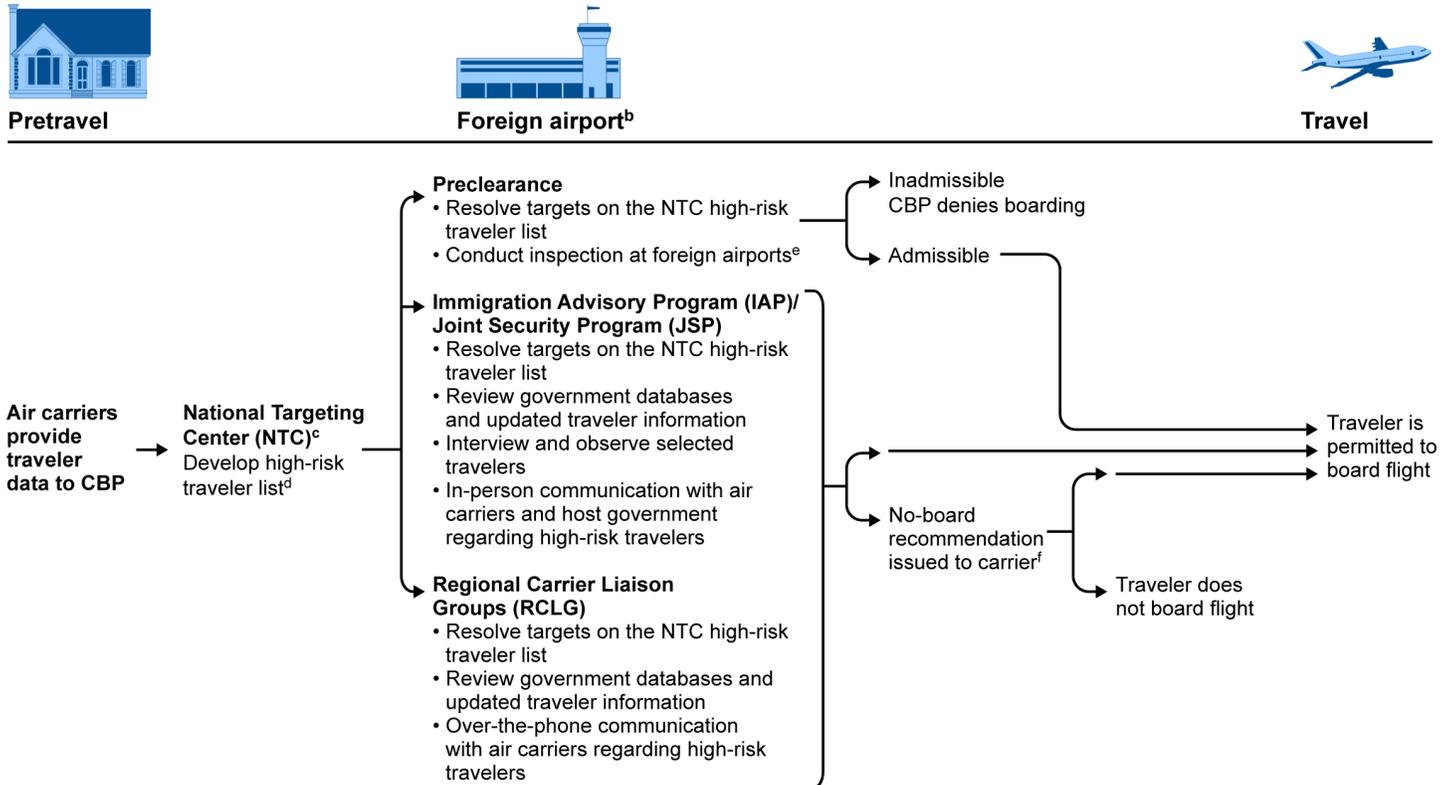
CBP's Air Predeparture Programs Interdict High-Risk Travelers on U.S.-Bound Flights, but CBP Has Not Evaluated Overall Effectiveness of Air Predeparture Programs

As we reported in January 2017, throughout the travel process, CBP's predeparture programs use the results of NTC's efforts to identify and interdict high-risk individuals destined for the United States while they are still overseas; however, we found that CBP had not evaluated the effectiveness of its predeparture programs as a whole, including implementing a system of performance measures and baselines to assess whether the programs are achieving their stated goals.¹³

CBP operates three air predeparture programs that are responsible for all U.S.-bound air travelers—Preclearance; the Immigration Advisory Program (IAP) and Joint Security Program (JSP); and the regional carrier liaison groups (RCLG). As we reported in January 2017, CBP data indicated that these programs identified and ultimately interdicted approximately 22,000 high-risk air travelers in fiscal year 2015, the most recent data available at the time of our review. Information on individuals who the NTC identifies through traveler data matching or rules-based targeting, including recurrent vetting, is compiled automatically through ATS into a daily high-priority list, or traveler referral list. CBP officers at the NTC review the traveler referral list for accuracy and to remove, if possible, any automatically generated matches determined to not be potential high-risk individuals. After this review, CBP officers at the NTC use ATS to send the traveler referral list to officers at each Preclearance, IAP, JSP, and RCLG location, as shown in figure 2.

¹³[GAO-17-216](#).

Figure 2: Actions Taken by U.S. Customs and Border Protection's (CBP) Predeparture Programs to Interdict High-Risk U.S.-Bound Air Travelers Throughout the Travel Process^a



Source: GAO analysis of CBP information. | GAO-17-599T

^aFor the purposes of this statement, the term travel process denotes the sequential steps that an international traveler takes to travel to the United States and focuses specifically on the points in time when travelers reserve and purchase airline tickets; check-in at the airport; transit to the United States; and arrive at a U.S.-based (i.e., domestic) airport. It does not focus on steps taken by the traveler before a ticket is reserved or purchased, such as obtaining a requisite travel authorization.

^bThis figure generally represents the actions CBP officers take to interdict high-risk travelers who will travel directly to the United States from a foreign last point of departure airport.

^cCBP's NTC leads all of CBP's predeparture targeting and vetting efforts. The NTC is a 24/7 operations entity within CBP's Office of Field Operations responsible for providing advance information and research about high-risk travelers and facilitating coordination between law enforcement and intelligence agencies in support of CBP's anti-terrorism mission and efforts to keep high-risk travelers from boarding U.S.-bound flights.

^dFor the purposes of this report, the term "high-risk traveler" refers to any traveler who may be inadmissible to the United States under U.S. immigration law or who may otherwise pose a threat to homeland or national security. See 8 U.S.C. § 1182 (establishing grounds for inadmissibility). According to CBP, the predeparture programs discussed in this report aim to interdict all high-risk travelers, but primarily focus on national security concerns and preventing known or suspected terrorists or travelers with connections to known or suspected terrorists from boarding flights destined for the United States.

^eCBP officers at air Preclearance locations conduct inspections of all U.S.-bound air travelers and determine whether they are admissible into the United States, as if conducted at a domestic U.S. port of entry.

^fIf CBP determines that a traveler at an RCLG, IAP, or JSP location will likely be deemed inadmissible upon arrival in the United States, CBP officers responsible for the location may recommend to the air carrier that it not board the traveler. Air carriers, however, retain authority to board the traveler unless, for example, the traveler has been identified by the Transportation Security Administration as being on the No Fly List, which is a subset of the Terrorist Screening Database that identifies individuals prohibited from boarding flights to, from, within, or overflying the United States.

Preclearance. Preclearance locations operate at foreign airports and serve as U.S. ports of entry. Preclearance operations began in 1952 in Toronto to facilitate trade and travel between the United States and Canada. As of January 2017, CBP operated 15 air Preclearance locations in six countries.¹⁴ Through the Preclearance program, uniformed CBP officers at a foreign airport exercise U.S. legal authorities to inspect travelers and luggage and make admissibility determinations prior to an individual boarding a plane to the United States.¹⁵ According to CBP officials, an inspection at a Preclearance location is the same inspection an individual would undergo at a domestic port of entry, and officers conducting Preclearance inspections exercise the same authority as officers at domestic ports of entry to approve or deny admission into the United States.¹⁶ As a result, travelers arriving at domestic air ports of entry from Preclearance locations do not have to be re-inspected upon entry.¹⁷ According to CBP data, in fiscal year 2015, CBP officers at Preclearance locations determined that 10,648 air travelers were inadmissible out of the approximately 16 million air travelers seeking admission to the United States through a Preclearance location. In addition to requiring that all travelers undergo a primary inspection, CBP

¹⁴See 19 C.F.R. § 101.5. CBP's Preclearance location in Victoria, Canada, only processes maritime travelers and, as a result, we did not include it in our January 2017 report. See [GAO-17-216](#).

¹⁵See 8 U.S.C. § 1103(a)(7); 19 U.S.C. § 1629. See also 8 C.F.R. §§ 235.1, 235.5; 19 C.F.R. §§ 148.22, 162.6, 162.8; and Preclearance Authorization Act of 2015, Pub. L. No. 114-125, tit. VIII, subtit. B, § 813, 130 Stat. 122, 217-18 (2016) (classified at 19 U.S.C. § 4432) (authorizing the Secretary of Homeland Security to establish and maintain CBP preclearance operations in a foreign country).

¹⁶Individuals denied admission to the United States at a Preclearance location are not permitted to proceed beyond the point of inspection and, thus, are unable to board a flight to the United States.

¹⁷According to CBP officials, in accordance with CBP's current preclearance agreements and processes, CBP officers retain the authority to inspect these travelers and their accompanying goods or baggage after arriving in the United States should further inspection be warranted.

officers in these locations also referred almost 290,000 individuals for secondary inspection.¹⁸

Immigration Advisory Program (IAP) and Joint Security Program (JSP). IAP and JSP operate at 9 and 2 foreign airports, respectively, as of January 2017. According to CBP officials, under this program, unarmed, plainclothes CBP officers posted at foreign airports partner with air carriers and host country government officials to help prevent terrorists and other high-risk individuals from boarding U.S.-bound flights by vetting and interviewing them before travel.¹⁹ According to CBP program documentation, CBP established IAP in 2004 to prevent terrorists, high-risk travelers, and improperly documented travelers from boarding airlines destined to the United States. Building on the IAP concept, CBP established JSP in 2009 to partner with host country law enforcement officials to identify high-risk travelers. CBP officers at IAP and JSP locations have the ability to question travelers and review their travel documents. They are to act in an advisory manner to the air carriers and host governments and do not have authority to deny boarding to individuals on U.S.-bound flights or fully inspect travelers or their belongings. IAP and JSP officers are authorized by CBP to make recommendations to airlines as to whether to board or deny boarding (known as a no-board recommendation) to selected travelers based on their likely admissibility status upon arrival to the United States. The final decision to board travelers, however, lies with the carriers. According to CBP data, CBP officers at IAP and JSP locations made 3,925 no-board recommendations in fiscal year 2015 for the approximately 29 million air travelers bound for the United States from such locations. During this

¹⁸Primary inspection refers to the procedure that CBP uses to conduct an initial inspection of individuals seeking to enter the United States to determine if additional review or scrutiny is needed to ensure compliance with U.S. law. Persons who need additional scrutiny and persons selected as part of a random selection process are subjected to a more detailed review called a secondary inspection. This involves, for example, a closer inspection of travel documents and possessions, additional questioning by CBP officers, and cross references through multiple law enforcement databases to verify the traveler's identity, background, purpose for entering the country, and other appropriate information.

¹⁹See 8 U.S.C. § 1225a(b).

same time period, CBP data indicated 1,154 confirmed encounters with individuals on the TSDB, including 106 on the No Fly List.²⁰

Regional Carrier Liaison Groups (RCLG). RCLGs are located and operate at three domestic airports—Miami International Airport, John F. Kennedy International Airport, and Honolulu International Airport. CBP established RCLGs in 2006 to assist air carriers with questions regarding U.S. admissibility requirements and travel document authenticity. According to CBP officials, RCLGs are responsible for coordinating with air carriers on all actionable referrals from NTC on U.S.-bound travelers departing from an airport without an IAP, JSP, or Preclearance presence. Each RCLG is assigned responsibility for travelers departing out of a specific geographic location.²¹ Similar to IAP and JSP, CBP officers in RCLGs also make no-board recommendations, as appropriate, to air carriers. CBP officers at RCLGs do not have authority to make admissibility determinations about U.S.-bound air travelers, and the final decision to board or not board a traveler lies with the carrier. CBP officers working at the three RCLGs made 7,664 no-board recommendations in fiscal year 2015 for the approximately 59 million travelers bound for the United States from locations within the RCLGs' spheres of responsibility. During this time period, CBP data indicated that RCLGs also reported 1,634 confirmed encounters with individuals in the TSDB, including 119 on the No Fly List.

In January 2017, we reported that CBP had not evaluated the effectiveness of its predeparture programs as a whole, including implementing a system of performance measures and baselines to assess whether the programs were achieving their stated goals.²² We reported that CBP had taken some initial steps to measure the performance of these programs. Specifically, CBP officials told us that they had collected a large quantity of data and statistics regarding the actions of their predeparture programs and had done so since program inception for all programs. However, due to changes in operational focus,

²⁰A confirmed encounter refers to when a representative of the U.S. government (in this case a CBP officer) comes into contact, either through physical interviewing or inspection or through electronic vetting, with an individual whose identity is confirmed as a match to a record in the TSDB. The No Fly List, which is a subset of the TSDB, identifies individuals prohibited from boarding flights to, from, within, or overflying the United States.

²¹RCLGs are not responsible for travelers departing from Preclearance locations.

²²[GAO-17-216](#).

technology updates, and the use of separate data systems at program locations, CBP had not collected consistent data across all of its predeparture programs. As a result, CBP did not have baseline data on which to measure program performance. However, CBP officials stated at the time that they had updated and uniform data collection systems that were consistent across all predeparture programs, which would enable CBP to identify performance baselines from fiscal year 2015 onward. According to senior CBP officials, some of the results of these programs were not easily measured. Officials also noted that relying on data alone may not always present the most accurate picture of the true impact of predeparture programs because changes to the travel process or other factors may impact the programs in ways that are not fully captured by the data. However, on the basis of our analysis of CBP's documentation, including official hearing statements, and interviews with program officials, we found that CBP used these data as indicators of the programs' success.

According to GAO's Program Evaluation Guide, which articulates best practices for program evaluation, a program evaluation is a systematic study using research methods to collect and analyze data to assess how well a program is working and why.²³ Moreover, consistent with requirements outlined in the Government Performance and Results Act of 1993 (GPRA), as updated by the GPRA Modernization Act of 2010, performance measurement is the ongoing monitoring and reporting of program accomplishments, particularly towards pre-established goals, and agencies are to establish performance measures to assess progress towards goals.²⁴ Agencies can use performance measurement to make various types of management decisions to improve programs and results, such as developing strategies and allocating resources, and identify problems and take corrective action. Therefore, we recommended that CBP develop and implement a system of performance measures and baselines for each program to help ensure that these programs are achieving their intended goals. By using data from fiscal year 2015, for

²³GAO, *Designing Evaluations: 2012 Revision*, [GAO-12-208G](#) (Washington, D.C.: January 2012). The best practices outlined in [GAO-12-208G](#) are based on GAO studies, policy documents, and program evaluation literature. To ensure the guide's competence and usefulness, drafts were reviewed by selected GAO, federal and state agency evaluators, and evaluation authors and practitioners from professional consulting firms.

²⁴See, generally, Pub. L. No. 103-62, 107 Stat. 285 (1993) (GPRA) and Pub. L. No. 111-352, 124 Stat. 3866 (2011) (updating GPRA). In particular, see 31 U.S.C. § 1115 (relating to agency performance plans and performance measurement).

example, to develop initial baselines, CBP could better measure program performance towards meeting stated goals. In response, CBP established a working group to develop and implement a system of performance measures and baselines to evaluate the effectiveness of CBP's predeparture programs. As of December 2016, the working group was gathering baseline data from fiscal year 2015 to compare with fiscal year 2016 data. In February 2017, CBP officials stated that the working group had identified potential performance measures but needs to further refine them. CBP officials stated that they expect to complete this work by the end of June 2017.

ICE Aims to Strengthen Screening of Visa Applicants through its Visa Security Program

The Homeland Security Act of 2002 authorized DHS to assign officers to each diplomatic and consular post at which visas are issued, and also authorized DHS to immediately assign personnel to Saudi Arabia to review all visa applications prior to final adjudication.²⁵ In response, DHS implemented the Visa Security Program (VSP) in 2003, and as of March 2016, ICE had established 26 visa security units in 20 countries. VSP aims to prevent terrorists and otherwise inadmissible travelers from attempting to enter the United States by screening visa applicants before the travel process begins. When reviewing applications for visas under VSP, ICE screens applicant information to identify applicants that potentially match records of individuals who are known or suspected threats to the United States or have immigration violations or derogatory information related to their criminal histories. In accordance with the Homeland Security Act of 2002, DHS officers assigned overseas are authorized to perform the following functions:

- provide expert advice and training to consular officers regarding specific security threats relating to the adjudication of individual visa applications or classes of applications,
- review any such visa applications either on the initiative of the employee of the department or at the request of a consular officer, or other persons charged with adjudicating such applications, and
- conduct investigations with respect to consular matters under the jurisdiction of the Secretary of Homeland Security.²⁶

²⁵Pub. L. No. 107-296, tit. IV, subtit. C, § 428(e), (i), 116 Stat. 2135, 2191 (classified at 6 U.S.C. § 236(e), (i)).

²⁶See 6 U.S.C. § 236(e)(2).

In March 2011, we reported, among other things, on DHS's efforts to expand VSP and challenges to VSP operations overseas.²⁷ For example, we found that training of consular officers by VSP agents varied from post to post, with some consular officers at some posts receiving no training. Therefore, we recommended that DHS issue guidance requiring ICE to provide training for consular officers. DHS concurred and issued guidance to enhance the training of consular officers by VSP offices abroad.

We also found that ICE did not gather comprehensive data on all the performance measures needed to evaluate the VSP mission objectives and that the data that ICE collected on VSP activities were limited by inconsistencies. Therefore, we recommended that ICE collect reliable data to allow it to accurately evaluate VSP performance. DHS did not concur with this recommendation and stated that VSP captured all the required performance metrics. However, as we reported, we determined that ICE was collecting some data on the required performance measures, but that the data were not sufficient to accurately demonstrate the progress made toward the program's stated objectives. We continue to believe that without collecting comprehensive data on performance measures, DHS cannot accurately demonstrate progress of VSP in enhancing national security. In addition, we found that VSP agents performed various investigative and administrative functions beyond their visa security responsibilities, which limited their time spent on visa security activities, and ICE did not track this information in its tracking system, making it unable to identify the time spent on investigative and administrative functions. Therefore, we recommended that ICE develop a mechanism to track the amount of time its agents spent on visa security activities and other investigations to determine appropriate staffing levels and resource needs for VSP operations. DHS did not concur with our recommendation and stated that ICE tracked case investigation hours through its case management system, and that adding the metric to the VSP tracking system would be redundant. However, we found at the time, according to ICE documentation, that ICE could not accurately determine the amount of time that VSP agents spent on investigative and visa security activities because ICE did not distinguish between the hours logged by VSP agents and hours logged by other ICE officials at posts abroad and that ICE did not maintain accurate data on the time VSP agents spent on visa security activities at posts.

²⁷ [GAO-11-315](#).

ICE did not take action to implement these recommendations and we continue to believe that it needs to take steps to address issues we identified. We have ongoing work assessing DHS, State, and other U.S. agency efforts to strengthen the security of the visa process, including oversight of VSP, in which we plan to follow up on the findings and recommendations from our March 2011 report related to ICE's efforts to enhance VSP performance measurement, among other things. We plan to report later this year on the results of this work.

All VWP Countries Have Entered into Information Sharing Agreements or Equivalents, but Not All Are Sharing Information as Required

In May 2016, among other things, we reported that all 38 countries participating in the VWP had entered into the three types of required information-sharing agreements, or their equivalents, to (1) report lost and stolen passports, (2) share identity information about known or suspected terrorists, and (3) share criminal history information.²⁸ However, we reported that not all countries had shared information through two of the agreements. Specifically, we reported that all VWP countries reported passport information through the first agreement, but about one-third of VWP countries were not sharing terrorist identity information through the second agreement and about one-third of the countries had not yet shared criminal history information through the third agreement. Although U.S. agencies receive law enforcement and national security information from VWP countries through other means, such as multilateral entities, the U.S. government identified the information-sharing agreements as critical for protecting the United States from nationals of VWP countries who might present a threat. For example, as we reported, information provided through HSPD-6 arrangements has enhanced U.S. traveler-screening capabilities and improved U.S. agencies' ability to prevent known and suspected terrorists from traveling to the United States. Prior to the December 2015 enactment of the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015, U.S. law required VWP countries to enter into, but did not specifically require that countries implement, the information sharing agreements. DHS announced in August 2015 that it had developed a new requirement that countries implement the agreements by sharing information.²⁹ However, as we reported, DHS had not specified time frames for working with VWP

²⁸GAO-16-498. In this statement, such required agreements are referred to as both agreements and arrangements.

²⁹See Pub. L. No. 114-113, div. O, tit. II, § 204(c)-(d), 129 Stat. at 2991-92 (requiring countries to fully implement information-sharing agreements in order to participate in the VWP); 8 U.S.C. § 1187(c)(2)(F).

countries to institute this and other new VWP security requirements. In May 2016, we recommended that DHS specify time frames for working with VWP countries to institute the additional VWP security requirements, including the requirement that the countries fully implement agreements to share information about known or suspected terrorists through the countries' HSPD-6 arrangements and PCSC agreements with the United States. DHS concurred with the recommendation and, as of April 2017, reported that officials are continuing to work with VWP countries on time frames for implementing program requirements.

Chairman Gallagher, Ranking Member Watson Coleman, and Members of the Task Force, this concludes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contact and Acknowledgments

For further information regarding this testimony, please contact Rebecca Gambler at (202) 512-8777 or gablerr@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this testimony are Kathryn H. Bernet, Assistant Director; Eric Hauswirth; Paul Hobart; Brandon Hunt; Hynek Kalkus; Thomas Lombardi; Sasan J. "Jon" Najmi; Erin O'Brien; Mary Pitts; and Garrett Riba.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [LinkedIn](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov and read [The Watchblog](#).

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.