



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.