DEPARTMENT OF STATE

WRITTEN STATEMENT

OF

DAVID T. DONAHUE

PRINCIPAL DEPUTY ASSISTANT SECRETARY FOR CONSULAR AFFAIRS

DEPARTMENT OF STATE

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

HEARING

ON

THE SECURITY OF U.S. VISA PROGRAMS

MARCH 15, 2016

Good morning Chairman Johnson, Ranking Member Carper, and distinguished Members of the Committee. The Department of State is dedicated to the protection of our borders. We have no higher priority than the safety of our fellow citizens at home and overseas. We and our partner agencies throughout the federal government have built a layered visa and border security screening system, and continue to refine and strengthen the five pillars of visa security: technological advances, biometric innovations, personal interviews, data sharing, and training.

This layered approach enables the Department of State to track and review the visa eligibility and status of foreign visitors from their visa applications to their entry into the United States. Lessons learned through the years have led to significant improvements in procedures and capabilities. At the same time, the tragic events in Paris and San Bernardino demonstrated the changing nature of threats and our obligation to constantly analyze, test, and update our clearance procedures. We will never stop doing so.

A Layered Approach to Visa Security

In coordination with interagency partners, the Department has developed, implemented, and refined an intensive visa application and screening process. We require personal interviews in most cases, including all immigrant and fiancé(e) cases, employ analytic interviewing techniques, and incorporate multiple biographic and biometric checks in the visa process. Underpinning the process is a sophisticated global information technology network that shares data among the Department and federal law enforcement and intelligence agencies. Security is our primary mission. Every visa decision is a national security decision. The rigorous security screening regimen I describe below applies to all visa categories.

All visa applicants submit online applications – the online DS-160 nonimmigrant visa application form, or the online DS-260 immigrant visa application form. Online forms enable consular and fraud prevention officers, and our intelligence and law enforcement partners, to analyze data in advance of the visa interview, including the detection of potential non-biographic links to derogatory information. The online forms offer foreign language support, but applicants must respond in English, to facilitate information sharing among the Department and other government agencies.

Consular officers use a multitude of tools to screen visa applications. No visa can be issued unless all relevant concerns are fully resolved. The vast majority of visa applicants are interviewed by a consular officer. During the interview, consular officers pursue case-relevant issues pertaining to the applicant's identity, qualifications for the particular visa category in question, and any information pertaining to possible ineligibilities related to criminal history, prior visa applications or travel to the United States, and/or links to terrorism or security threats.

As a matter of standard procedure, all visa applicant data is reviewed through the Department's Consular Lookout and Support System (CLASS), an online database containing approximately 36 million records of persons, including those found ineligible for visas and persons who are the subjects of potentially derogatory information, drawn from records and sources throughout the U.S. government. CLASS employs sophisticated name-searching algorithms to identify accurate matches between visa applicants and any derogatory information contained in CLASS. We also run all visa applicants' names against the Consular Consolidated Database (CCD, our automated visa application record system) to detect and respond to any derogatory information regarding visa applicants and visa holders, and to check for prior visa applications, refusals, or issuances. The CCD contains more than 181 million immigrant and nonimmigrant visa records dating back to 1998. This robust searching capability, which takes into account variations in spelling and naming conventions, is central to our procedures.

We collect 10-print fingerprint scans from nearly all visa applicants, except certain foreign government officials, diplomats, international organization employees, and visa applicants over the age of 79 or under the age of 14. Those fingerprints are screened against two key databases: first, the Department of Homeland Security's (DHS) IDENT database, which contains a biometric repository of available fingerprints of known and suspected terrorists, wanted persons, and those who have committed immigration violations; and second, the Federal Bureau of Investigation's (FBI) Next Generation Identification (NGI) system, which contains more than 75.5 million criminal history records.

All visa photos are screened against a gallery of photos of known or suspected terrorists obtained from the FBI's Terrorist Screening Center (TSC), and against visa applicant photos contained in the Department's CCD.

In 2013, in coordination with multiple interagency partners, the Department launched the "Kingfisher Expansion" (KFE) counterterrorism visa vetting system through the National Counterterrorism Center (NCTC). While the precise details of KFE vetting cannot be detailed in this open setting, KFE supports a sophisticated comparison of multiple fields of information drawn from visa applications against intelligence community and law enforcement agency databases in order to identify terrorism concerns. If a "red-light" hit is communicated to the relevant consular post, the consular officer denies the visa application and submits it for a Washington-based interagency Security Advisory Opinion (SAO) review by federal law enforcement and intelligence agencies. In addition to this KFE "red-light" scenario, consular officers are required to submit SAO requests in any case with applicable CLASS name check results, and for a variety of interagency-approved policies developed to vet travelers that raise security concerns, including certain categories of travelers with a particular nationality or place of birth. In any case in which reasonable grounds exist to question visa eligibility on security related grounds, regardless of name check results, a consular officer suspends visa adjudication and requests an SAO. Consular officers receive extensive training on the SAO process, which under the aforementioned circumstances, requires them to deny the visa per INA section 221(g) and submit the case for interagency review via an SAO for any possible security-related ineligibilities. The applicant is informed of the denial and that the case is in administrative processing. An applicant subject to this review may be found eligible for a visa only if the SAO process resolves all concerns.

DHS's Pre-adjudicated Threat Recognition and Intelligence Operations Team (PATRIOT) and Visa Security Program (VSP) provide additional law enforcement review of visa applications at designated overseas posts. PATRIOT is a pre-adjudication visa screening and vetting initiative that employs resources from DHS/Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and the Department of State. It was established to identify national security, public safety, and other eligibility concerns prior to visa

issuance. A team of agents, officers, and analysts from ICE and CBP perform manual vetting of possible derogatory matches.

PATRIOT works in concert with the Visa Security Units (VSU) located in more than 20 high-threat posts and we are working with ICE to deploy VSUs to more visa issuing posts as rapidly as available resources will support. ICE special agents assigned to VSUs provide on-site vetting of visa applications and other law enforcement support to consular officers. When warranted, DHS officers assigned to VSUs conduct targeted, in-depth reviews of individual visa applications and applicants prior to issuance, and recommend refusal or revocation of applications to consular officers. The Department of State works closely with DHS to ensure that no known or suspected terrorist inadvertently receives a visa or is admitted into our country. The Department of State has not and will not issue a visa for which the VSU recommends refusal.

Training

Consular officers are trained to take all prescribed steps to protect the United States and its citizens when making visa adjudication decisions. Each consular officer completes an intensive, six-week Basic Consular Course. This course features a strong emphasis on border security and fraud prevention, with more than 40 classroom hours devoted to security, counterterrorism, fraud detection, and visa accountability programs. Adjudicators receive extensive classroom instruction on immigration law, Department policy and guidance, and consular systems, including review of background data checks and biometric clearances.

Students learn about the interagency vetting process through briefings from the Bureau of International Security and Nonproliferation; Consular Affairs' (CA) Office of Screening, Analysis and Coordination; CA's Counterfeit Deterrence Laboratory; Diplomatic Security; and the DHS/ICE Forensic Document Laboratory.

In addition, officers receive in-depth interviewing and name check technique training, spending more than 30 classroom hours critiquing real consular interviews, debriefing role plays, and other in-class activities. Basic interviewing training includes instruction in techniques for questioning an applicant to elicit information relevant to assessing visa eligibility. Officers use verbal and non-

verbal cues to judge an applicant's credibility and the veracity of the applicant's story. They examine and assess documentation, including electronic application forms, internal background check information, passports, and required supporting documents during the interview.

Officers receive continuing education in all of these disciplines throughout their careers. All consular officers have top secret clearances, and most speak the language of the country to which they are assigned and receive training in the culture of the host country.

Visas Viper Program

U.S. missions overseas report information about foreign nationals with possible terrorist connections through the Visas Viper reporting program. Following the December 25, 2009, attempted terrorist attack on Northwest Flight 253, we strengthened the procedures and content requirements for Visas Viper reporting. Chiefs of Mission are responsible for ensuring that all appropriate agencies and offices at post contribute relevant information for Viper nominations. Visas Viper cables must include complete information about all previous and current U.S. visas. On December 31, 2009, we updated instructions regarding procedures and criteria used to revoke visas. We added specific reference to cases that raise security and other concerns to the guidance regarding consular officers' use of the authority to deny visa applications under section 214(b) of the Immigration and Nationality Act (INA), if the applicant does not establish visa eligibility to the satisfaction of the consular officer. Instruction in appropriate use of this authority has been a fundamental part of officer training for several years.

Continuous Vetting and Visa Revocation

Federal agencies have been matching new threat information against existing visa records since 2002. We have long recognized this function as critical to managing our records and processes. This system of continual vetting evolved as post-9/11 reforms were instituted, and is now performed in cooperation with the TSC, NCTC, FBI, DHS/ICE, and CBP's National Targeting Center (NTC). All records added to the Terrorist Screening Database (TSDB) and Terrorist Identities Datamart Environment (TIDE) are checked against the CCD to determine if there are matching visa records. Through the KFE process, we also have additional

information checked against classified holdings. While this obviously includes biographic data taken during the visa process, biometric data taken during the visa process is likewise available to interagency partners in their counterterrorism and law enforcement efforts. Vetting partners send these matches electronically to the Department of State, where analysts review the hits and flag cases for possible visa revocation. We have visa information sharing agreements under which we widely disseminate our data to other agencies that may need to learn whether a subject of interest has, or has ever applied for, a U.S. visa.

The Department of State has broad authority to revoke visas, and we use that authority widely to protect our borders. Cases for revocation consideration are forwarded to the Department of State's Visa Office by embassies and consulates overseas, NTC, NCTC, and other entities. As soon as information is established to support a revocation (i.e., information that surfaced after visa issuance that could lead to an ineligibility determination, or otherwise indicates the visa holder poses a potential threat), a "VRVK" entry code showing the visa revocation, and lookout codes indicating specific potential visa ineligibilities, are added to CLASS, as well as to biometric identity systems, and then shared in near-real time (within approximately 15 minutes) with the DHS lookout systems used for border screening. As part of its enhanced "Pre-Departure" initiative, CBP uses VRVK records, among other lookout codes, to recommend that airlines not board certain passengers on flights bound for the United States. Every day, we receive requests to review and, if warranted, revoke visas for aliens for whom new derogatory information has been discovered since the visa was issued. The Department of State's Operations Center is staffed 24 hours a day, seven days a week, to address urgent requests, such as when a potentially dangerous person is about to board a plane. In those circumstances, the Department of State can and does use its authority to revoke the visa immediately. We continue to work with our interagency partners to refine the visa revocation and associated notification processes.

Revocations are typically based on new information that has come to light after visa issuance. Because individuals' circumstances change over time, and people who once posed no threat to the United States can become threats, continuous vetting and revocation are important tools. We use our authority to revoke a visa immediately in circumstances where we believe there is an

immediate threat, regardless of the individual's location, after which we will notify the issuing post and interagency partners as appropriate. We are mindful, however, not to act unilaterally, but to coordinate expeditiously with our national security partners in order to avoid possible disruption of important investigations. In addition to the hundreds of thousands of visa applications we refuse each year, since 2001, the Department has revoked approximately 122,000 visas, based on information that surfaced following visa issuance, for a variety of reasons. This includes approximately 10,000 visas revoked for suspected links to terrorism. Terrorism-related visa revocations account for only .009 percent of the approximately 108 million visas we have issued since January 2001.

Going Forward

We face dangerous and adaptable foes. We are dedicated to maintaining our vigilance and strengthening the measures we take to protect the American public and the lives of those traveling to the United States. We will continue to apply state-of-the-art technology to vet visa applicants. While increasing our knowledge of threats, and our ability to identify and interdict those threats, the interagency acts in accordance with the rules and regulations agreed upon in key governance documents. These documents ensure a coordinated approach to our security and facilitate mechanisms for redress and privacy protection.

We are taking several measures to confront developing threats and respond to the despicable terrorist attacks in Paris and San Bernardino.

With our interagency partners, particularly DHS, we conducted a thorough review of our K-visa process. As we constantly do, we analyzed our current K-visa processes, including security vetting, to identify areas where we could improve. We are further exploring and implementing several adjustments and recommendations, especially in regard to our adjudication of cases with applicants from countries of concern. These adjustments and recommendations include, but are not limited to, working with the Department of State's Diplomatic Security Service to explore assigning additional Regional Security Officers in direct support of consular sections and visa adjudications; working with DHS to explore expanding the use of ICE's PATRIOT screening in certain countries of concern where it is not already present; and taking another opportunity to review prior K-

visa adjudications and our internal standard operating procedures to determine what we can learn and use to inform our processes and training.

Additionally, we are working closely with DHS and the interagency to explore and analyze the use of social media screening of visa applicants. In addition to learning from our DHS colleagues, we began a pilot exploration of social media screening at 17 posts that adjudicate K-visa applications and immigrant visa applications for individuals from countries of concern. We expect to learn a great deal from this pilot and are confident we will have a much better understanding of the implications of using social media vetting for national security and immigration benefits. At the same time, we continue to explore methods and tools that potentially could assist in this type of screening and potentially provide new methods to assess the credibility of certain information from applicants. We believe these endeavors will provide us insights to continue to ensure the visa process is as secure, effective, and efficient as possible.

Information sharing with trusted foreign partners is an area that has seen significant development in recent years. For example, "to address threats before they reach our shores," as called for by President Obama and the Prime Minister of Canada in their February 4, 2011, joint declaration, *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness*, the Departments of State and Homeland Security have implemented arrangements for systematic information sharing with Canada. The established processes provide for nearly real-time access to visa and immigration data through matching of fingerprints, as well as through biographic name checks for information that an applicant previously violated immigration laws, was denied a visa, or is a known or suspected terrorist. Canadian officers currently access the U.S. records of Syrian nationals seeking refugee resettlement in Canada, among other populations of visa and immigration applicants.

As part of our long-term strategic planning to improve efficiency and accuracy in visa adjudications, while ensuring we can meet surging visitor visa demand, we are investigating the applicability of advanced technology in data analysis, risk screening, and credibility assessment. Keeping abreast of high-tech solutions will help us reduce threats from overseas while keeping the United States open for business.

I assure you that the Department of State continues to refine its intensive visa application and screening process, including personal interviews, employing analytic interview techniques, incorporating multiple biographic and biometric checks, and interagency coordination, all supported by a sophisticated global information technology network. We look forward to working with the committee staff on issues addressing our national security in a cooperative and productive manner.