



DEPARTMENT OF STATE

WRITTEN STATEMENT

OF

MICHELE THOREN BOND

ASSISTANT SECRETARY FOR CONSULAR AFFAIRS

DEPARTMENT OF STATE

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HEARING

ON

TERRORIST TRAVEL:

VETTING FOR NATIONAL SECURITY CONCERNS

DECEMBER 17, 2015

Good morning Chairman Chaffetz, Ranking Member Cummings, 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 abroad. We and our partner agencies throughout the federal government have built a layered visa and border security screening system. We 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 us and our interagency partners to track and review the visa eligibility and status of foreign visitors from their visa applications throughout their travel to, sojourn in, and departure from the United States. The lessons learned over the past several years have not been ignored. At the same time, the tragic events that transpired most recently in Paris and San Bernardino have demonstrated that no system is perfect. We must constantly analyze, test, and update our clearance procedures.

A Layered Approach to Visa Security

The Department has developed, implemented, and refined an intensive visa application and screening process, requiring personal interviews in most cases, including all immigrant and fiancé cases, employing analytic interview techniques, and incorporating multiple biographic and biometric checks. This process is supported by 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. Although recent events have sparked particular interest in the K-1 fiancé(e) visa, 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, as well as 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 applicants' data are reviewed through the Department's Consular Lookout and Support System (CLASS), our online database containing nearly 36 million records of persons found ineligible for visas, or against whom potentially derogatory information exists, drawn from records and sources throughout the U.S. government. CLASS employs sophisticated name-searching algorithms to find 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. The CCD contains more than 181 million immigrant and nonimmigrant visa records going back to 1998. The automated CLASS search algorithm runs the names of all visa applicants against the CCD to check for prior visa applications, refusals, or issuances. This robust searching capability, which takes into account variations in spelling, is central to our procedures.

We collect 10-print fingerprints from nearly all visa applicants, except certain foreign government officials, diplomats, international organization employees and visa applicants over the age of 79 or under 14. Those fingerprints are screened against two key databases. First, the Department of Homeland Security's (DHS) IDENT database, which contains a watchlist of available fingerprints of known and suspected terrorists, wanted persons, and immigration law violators. Second, the Federal Bureau of Investigation's (FBI) Next

Generation Identification (NGI) system, which contains more than 75.5 million criminal history records.

In addition, 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 the entire gallery of 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. KFE supports a sophisticated comparison of multiple fields of information drawn from applicants' visa applications against the totality of the information in U.S. government holdings. While the precise details of KFE vetting cannot be discussed in this open setting, the program screens all visa applicants against U.S. government terrorist identity databases. If a "red-light" hit is communicated to the relevant consular post, the consular officer suspends visa processing and submits the application for a Washington-based interagency Security Advisory Opinion (SAO) review by federal law enforcement and intelligence agencies. Consular officers receive extensive training on the SAO process, which requires them to issue a preliminary denial of a pending visa application and suspend further action, pending interagency review of any case with possible security ineligibilities.

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 individual 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 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 over twenty high-threat posts and is being deployed 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 to the maximum possible extent that no known or suspected terrorist 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 Counterfeit Deterrence Laboratory; Diplomatic Security; and Department of Homeland Security's Immigration and Customs Enforcement Forensic Document Laboratory.

In addition, officers receive in-depth interviewing and name-checking technique training, spending more than 30 classroom hours critiquing real consular interviews recorded abroad, and 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 determine 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 clearance, 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

Embassies and consulates report information on 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 guidance on consular officers' use of the authority to deny visas 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

The Department has 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. All records added to the Terrorist Screening Database are checked against the CCD to determine if there are matching visa records. Matches are sent electronically from the Department to TSC, where analysts review the hits and flag cases for possible visa revocation. We widely disseminate our data to other

agencies that may wish to learn whether a subject of interest has, or has ever applied for, a U.S. visa.

The Department has broad and flexible authority to revoke visas, and we use that authority widely to protect our borders. Cases for revocation consideration are forwarded to the Department by consular officers overseas, CBP's National Targeting Center (NTC), the National Counterterrorism Center and other entities. As soon as information is established to support a revocation (i.e., information that could lead to an inadmissibility determination), a "VRVK" entry code showing the visa revocation is added to CLASS, as well as to biometric identity systems, and then shared in near-real time (within about 15 minutes) with the DHS lookout systems used for border screening. As part of its enhanced "Pre-Departure" initiative, CBP uses VRVK records, among other lookout codes, to recommend that airlines not board certain passengers on flights bound for the United States. Almost every day, we receive requests to review and, if warranted, revoke any outstanding visas for aliens for whom new derogatory information has been discovered since the visa was issued. Our Operations Center is staffed 24 hours a day, 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 can and does use its authority to revoke the visa immediately, and thus prevent boarding.

Most revocations are based on new information that has come to light after visa issuance. Because individuals' circumstances change over time, and people who once posed no threat to the United States can become threats, 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. At the same time, we believe it is important not to act unilaterally, but to coordinate expeditiously with our national security partners in order to avoid possibly disrupting important investigations. Since 2001, the Department has revoked approximately 122,000 visas for a variety of reasons, including nearly 9,500 for suspected links to terrorism.

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 as well as facilitating mechanisms for redress and privacy protection.

We are taking several measures to confront developing threats and respond to the despicable terrorist attacks in San Bernardino and Paris. With our interagency partners, including DHS and the FBI, we have launched a senior-level review of the K-1 fiancé(e) visa process, cognizant of the probability that recommendations relevant to that category may apply to other visa types as well. It is too early to say what those recommendations may be, but this review is a top priority for us as we seek continuous improvements of our processes. Additionally, we are working with DHS and State's Bureau of Counterterrorism on both the security screening of Visa Waiver Program (VWP) travelers, and on enhancing the data sharing commitments required for VWP membership.

As part of our long-term strategic planning to improve efficiency and accuracy in visa adjudication, despite surging visitor 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 abroad while keeping the U.S. economy open for business.

I assure you that the Department continues to refine its intensive visa application and screening process requiring personal interviews, employing analytic interview techniques, incorporating multiple biographic and biometric checks, and interagency coordination, all supported by a sophisticated global information technology network.

Thank you. I look forward to your questions and comments.