



DEPARTMENT OF STATE

STATEMENT

OF

DAVID T. DONAHUE

DEPUTY ASSISTANT SECRETARY OF STATE FOR VISAS,

DEPARTMENT OF STATE

BEFORE THE

HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

HEARING

ON

VISA SECURITY AND PASSENGER PRE-SCREENING EFFORTS

IN THE WAKE OF FLIGHT 253

MARCH 11, 2010

Chairman Cuellar, Ranking Member Souder and distinguished Members of the Subcommittee, thank you for the opportunity to address you today.

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

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

In the case of Umar Farouk Abdulmutallab, on the day following his father's November 19, 2009 visit to the Embassy, we sent a cable to the Washington intelligence and law enforcement community through the Visas Viper system that "Information at post suggests [that Abdulmutallab] may be involved in Yemeni-based extremists." At the same time, the Consular Section entered Abdulmutallab into the Consular Lookout and Support System database known as CLASS, against which all visa applications are screened. In sending the Visas Viper cable and checking State Department records to determine whether Abdulmutallab had a visa, Embassy officials misspelled his name, but entered it correctly into CLASS. As a result of the misspelling in the cable, information about previous visas issued to him and the fact that he held a valid U.S. visa at that time, was not included in the cable. The CLASS entry using the correct spelling resulted in a lookout that was shared automatically with the primary lookout system used by the Department of Homeland Security (DHS) and accessible to other partner agencies. DHS has noted that, as a result of that record, they planned to meet Abdulmutallab and question him upon arrival.

We took immediate action to improve the procedures and content requirements for Visas Viper cable reporting that will call attention to the visa application and issuance information that is already part of the data that we share with our national security partners. All officers have been instructed to include complete information about all previous and current U.S. visa(s) when a Visas Viper cable is sent. This instruction includes guidance on specific methods to comprehensively

and intensively search the database of visa records by conducting a wide-parameter, “fuzzy search,” leveraging an existing search capability called “Person Finder,” when searching our comprehensive repository of visa records in the Consular Consolidated Database (CCD). Searches conducted in this manner will identify visa records despite variations in the spelling of names as well as in dates of birth, places of birth, and nationality information.

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

The Department of State has been matching new threat information with our records of existing visas since 2002. We have long recognized this function as critical to the way we manage our records and processes. This system of continual vetting has evolved as post 9/11 reforms were instituted and is now performed by the Terrorist Screening Center (TSC). All records added to the Terrorist Screening Database are checked against the Department’s Consolidated Consular Database (CCD) to determine if there are matching visa records. Matches are sent

electronically from the TSC to the Department of State to flag cases for possible visa revocation. In addition, we have widely disseminated our data to other agencies that may wish to learn whether a subject of interest has a U.S. visa. Cases for revocation consideration are forwarded to us by our consular offices overseas, our domestic visa office, DHS/Customs and Border Protection's (CBP) National Targeting Center (NTC), and other entities. Almost every day, we receive requests to review and, if warranted, revoke visas for potential travelers for whom new derogatory information has been discovered since the visa was issued. Our Operations Center is staffed 24 hours per day/7 days per week to address urgent requests, such as when the person is about to board a plane. I frequently use the State Department's authority to prudentially revoke the visa and prevent boarding.

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

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

We have been actively using this revocation authority as we perform internal reviews of our data against watchlist information provided by partner agencies. For example, we are re-examining information in our CLASS database regarding individuals with potential connections to terrorist activity or support for such activity. We are reviewing all previous Visas Viper submissions and cases that other agencies are bringing to our attention from the No Fly and Selectee lists, as well as other sources. In these reviews, we identified cases for revocation and we also confirmed that substantial numbers of individuals in these classes hold no visas and of those few who did, a great many were revoked prior to the current review. We recognize the gravity of the threat we face and are working intensely with our colleagues from other agencies with the desired goal that when the U.S. Government obtains information, no person who may pose a threat to our security, holds a valid visa.

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

Finally, the Department is reviewing the procedures and criteria used in the field to revoke visas and will issue new instructions to our officers. Revocation

recommendations will be added as an element of reporting through the Visas Viper channel. We are in the process of providing additional guidance to the field on use of the broad authority of visa officers to deny visas on security and other grounds. Instruction in appropriate use of this authority has already been a fundamental part of officer training for years.

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

We are the first line of defense in border security. Our global presence, foreign policy mission and personnel structure give us singular advantages in executing the visa function throughout the world. Our authorities and responsibilities enable us to provide a global perspective to the visa process and its impact on U.S. national interests. The issuance and refusal of visas has a direct impact on our foreign relations. Visa policy quickly can become a significant bilateral problem that harms broader U.S. interests if handled without consideration for foreign policy impacts. The conduct of U.S. visa policy has a direct and significant impact on the

treatment of U.S. citizens abroad. The Department of State is in a position to anticipate and weigh all those factors. Remember, the vast majority of the more than two million visas denied last year were denied for reasons unrelated to terrorism. Let me reiterate, however, that the Department of State is fully committed to protecting our borders and has no higher priority than the safety of our fellow citizens and the legitimate foreign visitors who contribute so much to our economy and society.

The State Department has developed and implemented intensive screening processes requiring personal interviews, employing analytic interview techniques, incorporating multiple biometric checks, all built around a sophisticated global information technology network. We have visa offices present in virtually every country of the world, staffed by consular officers drawn from the Department's professional, and mobile multilingual Foreign Service Officer workforce. These officials are dedicated to a career of worldwide service, and they provide the cultural awareness, knowledge and objectivity to ensure that the visa function remains the frontline of border security. Each officer's experience and individual skill-set contribute to an overall understanding of the political, legal, economic, and cultural development of foreign countries in a way that gives the Department of State a special expertise over matters directly relevant to the full range of visa ineligibilities.

Consular officers are trained to take all necessary steps to protect the United States and its citizens during the course of making a decision on a visa application. Each

consular officer is required to complete the Department's Basic Consular Course at the National Foreign Affairs Training Center prior to performing consular duties. The course places strong emphasis on border security, featuring in-depth interviewing and name-checking technique training, as well as fraud prevention. Consular officers receive continuing education, including courses in analytic interviewing, fraud prevention and advanced security name-checking.

Consular officers refused 2,181,986 nonimmigrant and immigrant visas in FY2009 out of 8,454,936 applications. We now are renewing guidance to our officers on their authority to refuse visas with specific reference to cases that raise security concerns. No visa is issued without it being run through security checks against our interagency law enforcement and intelligence partners' data. And we screen applicants' fingerprints against U.S. databases as well. The results of these checks by consular officers and any fraud indicators are brought to the attention of VSU officers wherever they are posted abroad.

In addition, the Department of State's Security Advisory Opinion (SAO) mechanism provides officers with the necessary advice and background information to adjudicate these cases of visa applicants with possible terrorism ineligibilities. Consular officers receive extensive training on the SAO process, including namechecking courses that assist in identifying applicants requiring additional Washington vetting. The SAO process requires the consular officer to suspend visa processing pending interagency review of the case and additional guidance. Most SAOs are triggered by clear and objective circumstances, such as nationality, place of birth, residence or visa name check results. In addition, in

cases where reasonable grounds exist, regardless of name check results, to suspect that an applicant may be inadmissible under the security provisions of the Immigration and Nationality Act, consular officers suspend processing and institute SAO procedures.

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

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

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

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

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

Working in concert with DHS, we proactively expanded biometric screening programs and integrated this expansion into existing overseas facilities. In partnership with DHS and the Federal Bureau of Investigation (FBI), we established the largest biometric screening process on the globe. We were a pioneer in the use of facial recognition techniques and remain a leader in operational use of this technology. In 2009, we expanded use of facial recognition from a selected segment of visa applications to all visa applications. We now are expanding our use of this technology beyond visa records. We are testing use of iris recognition technology in visa screening, making use of both identity and derogatory information collected by DOD. These efforts require intense ongoing cooperation from other agencies. We successfully forged and continue to foster partnerships that recognize the need to supply accurate and speedy screening in a 24/7 global environment. As we implement process and policy changes, we are always striving to add value in both border security and in operational results. Both dimensions are important in supporting the visa process.

In addition, we have 145 officers and 540 locally employed staff devoted specifically to fraud prevention and document security, including fraud prevention officers at overseas posts. We have a large Fraud Prevention Programs office in Washington, D.C., that works very closely with the Bureau of Diplomatic Security, and we have fraud screening operations using sophisticated database checks at both the Kentucky Consular Center and the National Visa Center in Portsmouth, New Hampshire. Their role in flagging applications and applicants who lack credibility, who present fraudulent documents, or who give us false information adds a valuable dimension to our visa process.

The Bureau of Diplomatic Security adds an important law enforcement element to the Department's visa procedures. There are currently 75 Assistant Regional Security Officer Investigator (ARSOIs) positions approved for 73 consular sections overseas specifically devoted to maintaining the integrity of the process. This year, the Bureau of Diplomatic Security has approved 48 additional ARSOI positions to work in consular sections overseas. They are complemented by officers working domestically on both visa and passport fraud criminal investigations and analysis. These highly trained law enforcement professionals add another dimension to our border security efforts.

The multi-agency team effort on border security, based upon broadly shared information, provides a solid foundation. At the same time we remain fully committed to correcting mistakes and remedying deficiencies that inhibit the full and timely sharing of information. We have and we will continue to automate processes to reduce the possibility of human error. We fully recognize that we

were not perfect in our reporting in connection with the attempted terrorist attack on Flight 253. We are working and will continue to work not only to address that mistake but to continually enhance our border security screening capabilities and the contributions we make to the interagency effort.

We believe that U.S. interests in legitimate travel, trade promotion, and educational exchange are not in conflict with our border security agenda and, in fact, further that agenda in the long term. Our long-term interests are served by continuing the flow of commerce and ideas that are the foundations of prosperity and security. Acquainting people with American culture and perspectives remains the surest way to reduce misperceptions about the United States. Fostering academic and professional exchange keeps our universities and research institutions at the forefront of scientific and technological change. We believe the United States must meet both goals to guarantee our long-term security.

We are facing an evolving threat. The people and the tools we use to address this threat must be sophisticated and agile and must take into account the cultural and political environment in which threats arise. The people must be well-trained, motivated and knowledgeable. Information obtained from these tools must be comprehensive and accurate. Our criteria for taking action must be clear and coordinated. The team we use for this mission must be the best. The Department of State has spent years developing the tools and personnel needed to properly execute the visa function overseas and remains fully committed to continuing to fulfill its essential role on the border security team.