PennState Law Center for Immigrants' Rights Clinic

MaggioKattar

To: Interested Parties
From: Shoba Sivaprasad Wadhia and Anna Gallagher
Re: Administrative Processing: FOIA Response from Department of State
Date: July 6, 2017

In April 2014, the Center for Immigrants' Rights Clinic (on behalf of Maggio & Kattar) filed a FOIA request seeking information about the Department of State's Administrative Processing Program. This same year, we researched and prepared a "Frequently Asked Questions" document that is available here.

Administrative processing, also known as Security Advisory Opinion (SAO), is the time period during which visa applications undergo additional review outside of the "normal" visa processing times. Administrative processing takes place after the visa interview. The topic of Administrative Processing pre-dates the current administration but has become more relevant as plans for "extreme vetting" and restrictions on travel surface.

On June 29, 2017, and following an email and telephonic exchange with the Department of State's (DOS) FOIA office to narrow scope of the request, we received the following response from DOS. These materials are attached to this memo and to our knowledge, represent the largest set of records from DOS on the topic.

1. Five instances of congressional testimony by the Consular Affairs Bureau (CA) for the past three years (beginning May 1, 2014) discussing SAOs.
2. A document identifying where visa applicants and their representatives should direct various types of questions relating to pending visa applications, including questions about cases pending in administrative processing.
3. A detailed description of the functions of the office responsible for administrative processing of SAOs.
4. The total number of SAOs for years 2012 – 2017. During this time period, there were more than 850,000 SAOs. Currently, 34,681 SAOs are open.
5. As to whether information on administrative processing is reported, and if so to whom.
6. Any outcomes goals, quotas or requirements relating to administrative processing and/or SAO.
7. A report reflecting SAOs broken down by nationality and visa category for each year 2012 – 2016. Among the top nationalities processed for SAOs were: India, Iran, Pakistan, China and Saudi Arabia (and in more recent years, Russia). Among the top visa categories subject to SAOs were: B1/B2, F1, J1, A2, and H1B.

From: Smith, Michelle L [mailto:SmithML4@state.gov]
Sent: Thursday, June 29, 2017 3:46 PM
To: Wadhia, Shoba
Subject: FW: FOIA Request F-2014-06832 (April 15, 2014)

Good Afternoon Ms. Wadhia,

Please find attached a final response letter and documents that are responsive to your request. Should you have any questions or concerns, please visit us at www.travel.state.gov or contact me at any time. Thank you.

Best regards,

Michelle L. Smith
Visa Liaison Officer
Contractor, Quality Support, Inc.
U.S. Department of State
Bureau of Consular Affairs
CA/VO/L/A, 12.522D
600 19th Street, N.W.
Washington, DC 20520
Office (202) 485-7633

smithML4@state.gov

This email is UNCLASSIFIED.

From: Brault, Steven F
Sent: Thursday, June 29, 2017 3:27 PM
To: Smith, Michelle L
Subject: FW: FOIA Request F-2014-06832 (April 15, 2014)

Official
UNCLASSIFIED

From: Wadhia, Shoba [mailto:ssw11@dsl.psu.edu]
Sent: Sunday, May 07, 2017 1:55 PM
To: Newman, David S; 'agallagher@maggio-kattar.com'
Cc: Brault, Steven F; 'ssw11@psu.edu'
Subject: RE: FOIA Request F-2014-06832 (April 15, 2014)

Dear Mr. Newman.

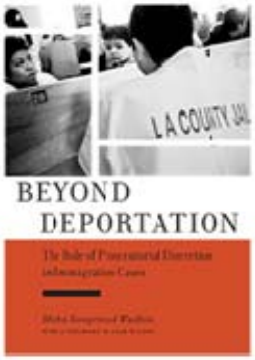
The information you marked in red is consistent with our most recent discussion and would satisfy our April 15, 2014 FOIA request.

Thank you very much. We look forward to receiving the information.

Sincerely, Shoba Sivaprasad Wadhia and Anna Gallagher

Shoba Sivaprasad Wadhia, Esq.
Samuel Weiss Faculty Scholar &
Clinical Professor of Law
Director, Center for Immigrants' Rights Clinic
Penn State Law
The Pennsylvania State University
329 Innovation Blvd., Suite 118
University Park, PA 16802
Office: 814-865-3823|Email: ssw11@psu.edu |Twitter: @shobawadhia| Medium
Faculty Page: www.pennstatelaw.psu.edu/faculty/wadhia
Post-Election Immigration Resources: https://pennstatelaw.psu.edu/immigration-after-election
Articles on SSRN: http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=1035598
Book Website: www.beyonddeportation.com

Author of *Beyond Deportation: The Role of Prosecutorial Discretion in Immigration Cases*, available in paperback, May 2017



From: Newman, David S [mailto:NewmanDS@state.gov]
Sent: Saturday, May 6, 2017 6:13 AM
To: Wadhia, Shoba <ssw11@dsl.psu.edu>; 'agallagher@maggio-kattar.com' <agallagher@maggio-kattar.com>
Cc: Brault, Steven F <BraultSF@state.gov>
Subject: FOIA Request F-2014-06832 (April 15, 2014)

Shoba and Anna,

We provide this as follow-up to our conversation of April 28, 2017, regarding your above-referenced FOIA request. We have copied below each of the requests in your "Request for Information" and interspersed our responses in red, in the conditional tense, reflecting what we would be prepared to provide in full satisfaction of the above-referenced request, should we reach agreement on this basis.

Request for Information

1. Any correspondence and/or other documents maintained by the Department of State (DOS) since January 1, 2012 which relate or refer in any manner to administrative processing and/or SAO, including but not limited to:

   a. Internal DOS memoranda, communications and other written guidance or goals regarding administrative processing and/or SAO, including protocols and procedures for placing an applicant's case in administrative processing;
   b. Training materials, including but not limited to power points, manuals, instructions, orders, outlines and reading material relating to administrative processing and/or SAO;

   As discuss on April 28, 2017, we understand this request now is limited to Security Advisory Opinions (SAOs), to the exclusion of other forms of administrative processing unrelated to security concerns. The substantive portions of the responsive documents are not releasable. We believe the most comprehensive information releasable on this subject is in congressional testimony. We searched all instances of congressional testimony by the Consular Affairs Bureau for the past three years (beginning May 1, 2014), and located five instances of testimony discussing SAOs (listed on the attachment) from 2015, 2016, and 2017 that we would be prepared to provide. As discussed, we also will provide a document identifying where visa applicants and their representatives should direct various types of questions relating to pending visa applications, including questions about cases pending in administrative processing.

c. Documents designating the DOS divisions that are involved in administrative processing and/or SAO, including information on but not limited to:

i. Employee(s)' job title;
ii. Duties of personnel;
iii. Number of personnel

We would provide a detailed description of the functions of the responsible office, but it would not include the details listed above.

d. Documents relating to the monitoring or supervision of administrative processing and/or SAO, including information on but not limited to:

i. Number of people actively in administrative processing;
ii. Number of people that have undergone administrative processing;

We would create and provide reports with the number of SAOs (not people) described in items (i) and (ii), above, for years 2012 – 2016.

iii. The DOS division(s) that are responsible for monitoring the progress of cases placed in administrative processing;

We would provide a detailed description of the functions of the responsible office.

iv. Whether information on administrative processing is reported, and if so to whom;

We would respond in writing to this request.

v. Whether reports on administrative processing are mandatory or optional;

We would respond in writing to this request.

vi. How often reports on administrative processing are generated;

We would respond in writing to this request.

e. Any outcomes goals, quotas or requirements relating to administrative processing and/or SAO.

We would respond in writing to this request relative to goals and quotas. Information and documents discussing requirements are not releasable.

2. Records from DOS databases for all cases where administrative processing was requested or ordered. For each case identified, please provide the following information:

a. Applicant's country of origin;
b. Applicant's gender;
c. Applicant's age;
d. Requested visa category;
e. Grounds triggering administrative processing;
f. Length of time in administrative processing;
g. Outcome of SAO (visa approval or visa denial);
h. Grounds for visa denial (if applicable).

In an email of May 4, 2015, from Shoba Wadhia to Lynne Martin, requesters clarified section 2 of the FOIA request stating:

> I would like to clarify that we are not requesting individual files of persons who are or have been placed in administrative processing. Instead, we want to have a better understanding of who is placed in administrative processing by gender, age, nationality, etc. Thus, we request demographic information and numbers of individuals who have been placed in administrative processing as per our request.

Individual visa records are not releasable and we do not have existing documents with responsive statistics, as described in the clarification of May 4, 2015. In response to section 2 of the request, as modified, we would provide the following:

- A report we create for this purpose reflecting SAOs broken down by nationality of visa applicant for each year 2012 – 2016.
- A report we create for this purpose reflecting SAOs broken down by visa classification for each year 2012 – 2016.
- A report we create for this purpose showing the percentage of SAOs closed within 60 days for each of the years 2012-2016.
- The number of visas denied under section 212(a)(3)(B) for each of the years 2012 – 2016.

- A statement as to whether an SAO is required before a visa may be denied under INA section 212(a)(3)(B).

As discussed, we would endeavor to transmit all items to you within 60 days of receiving a response from you stating that you will deem our submission of the documents and information we describe above as fully satisfying your above-referenced FOIA request.

Sincerely,
David S Newman
Director of Legal Affairs, Visa Office
Bureau of Consular Affairs
US Department of State
(o) (202) 485-7583
(c) (202) 812-5820

Official
UNCLASSIFIED

From: Wadhia, Shoba [mailto:ssw11@dsl.psu.edu]
Sent: Tuesday, April 18, 2017 6:40 AM
To: Brault, Steven F
Cc: agallagher@maggio-kattar.com
Subject: Re: FOIA requests for SAO-related documents

Steve vat this point 2pm Friday works best. Thank you. Sincerely,

Shoba Sivaprasad Wadhia Esq.
Samuel Weiss Faculty Scholar
Clinical Professor and Director
Center for Immigrants' Rights
Penn State Law
http://pennstatelaw.psu.edu/faculty/wadhia
Confidentiality fully enforced.
Sent from my iPad

On Apr 18, 2017, at 6:38 AM, Wadhia, Shoba <ssw11@dsl.psu.edu> wrote:

> Dear Steven. How is next Friday at 11am or 2pm? Thank you. Sincerely,

Shoba Sivaprasad Wadhia Esq.
Samuel Weiss Faculty Scholar
Clinical Professor and Director
Center for Immigrants' Rights
Penn State Law
http://pennstatelaw.psu.edu/faculty/wadhia
Confidentiality fully enforced.
Sent from my iPad

On Apr 17, 2017, at 10:38 AM, Brault, Steven F <BraultSF@state.gov> wrote:

> Dear Professor Shoba,
>
> Thank you for your response which Director Newman passed to me for follow-up. We do think further conversation on how the State Department might be able to assist with your FOIA request may prove fruitful. Director Newman wants me to participate in his call with you and, since I will be out of the office this Friday, we are hoping that we can arrange an alternative date during the following week.
>
> Are there specific days/times next week (other than Wednesday which is already booked full with meetings) that are good for you?
>
> Best regards,
>
> Steve Brault
> FOIA Coordinator
> CA/VO/L
> 703-485-3640
>
> **Official**
> **UNCLASSIFIED**
>
> ---
>
> **From:** Wadhia, Shoba <ssw11@dsl.psu.edu>
> **Sent:** Friday, April 14, 2017 9:05 AM
> **To:** Newman, David S; 'ssw11@psu.edu'
> **Cc:** 'Anna Gallagher (agallagher@maggio-kattar.com)'
> **Subject:** RE: FOIA requests for SAO-related documents
>
> Dear Mr. Newman: Thank your email. We are absolutely interested in receiving any information that is unclassified. I have already had a few conversations with FOIA staff at DOS (over the past nearly three years since we filed this request) about the scope and thus a bit surprised there are still outstanding questions. We are available to speak with you on **Friday, April 21.** Please confirm if there are time slots that might work for you? Thank you very much.
>
> Sincerely, Shoba
>
> Shoba Sivaprasad Wadhia, Esq.
> Samuel Weiss Faculty Scholar &
> Clinical Professor of Law
> Director, Center for Immigrants' Rights Clinic

Penn State Law
The Pennsylvania State University
329 Innovation Blvd., Suite 118
University Park, PA 16802
Office: 814-865-3823|Email: ssw11@psu.edu |Twitter: @shobawadhia| Medium
Faculty Page: www.pennstatelaw.psu.edu/faculty/wadhia
Post-Election Immigration Resources: https://pennstatelaw.psu.edu/immigration-after-election
Articles on SSRN: http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=1035598
Book Website: www.beyonddeportation.com

Author of *Beyond Deportation: The Role of Prosecutorial Discretion in Immigration Cases*, available in paperback, May 2017

From: Newman, David S [mailto:NewmanDS@state.gov]
Sent: Saturday, April 8, 2017 10:17 PM
To: 'ssw11@psu.edu' <ssw11@psu.edu>
Subject: FOIA requests for SAO-related documents

Dear Professor Shoba Sivaprasad Wadhia,

The attached FOIA request was brought to my attention. It is dated April 15, 2014. I will assume you have a continuing interest in pursuing the request, unless you advise otherwise.

As you might expect, much of the information you seek is protected from disclosure, as it relates to sensitive security screening procedures involving federal intelligence and law enforcement agencies. If your objective in pursuing the FOIA request is to receive as much releasable information as possible to address specific questions you may have, then I believe a conversation between our offices could be constructive. I would be prepared to speak with you, joined by members of my staff best positioned to address your questions and follow up with the production of relevant documents. I trust you understand that the laws exempting certain information from FOIA requests similarly prohibit us from disclosing the information to you.

I will be out of the office the week of October 10-14, 2017, but if you are interested in pursuing such a conversation, please send me a note with preferred dates and we will work to arrange it.

Sincerely,
David S Newman
Director of Legal Affairs, Visa Office
Bureau of Consular Affairs
US Department of State
Washington, DC 20006

United States Department of State

Washington, D.C. 20520

Shoba Sivaprasad Wadhia
Director, Center for Immigrants' Rights
Pennsylvania State University
Dickinson School of Law
329 Innovation Boulevard, Ste. 118
State College, PA 16803

June 29, 2017

Case Control Number: F-2014-06832

Dear Ms. Wadhia:

As discussed on April 28, 2017, and confirmed by your email of May 7, 2017, this response constitutes the Department's full satisfaction of the above-referenced FOIA request. Per the referenced communications, the request now is limited to Security Advisory Opinions (SAOs), to the exclusion of other forms of administrative processing unrelated to security concerns.

The following describes the items we agreed to provide, with the responsive information included or appended as attachments.

1. Five instances of congressional testimony by the Consular Affairs Bureau (CA) for the past three years (beginning May 1, 2014) discussing SAOs (attached).

2. A document identifying where visa applicants and their representatives should direct various types of questions relating to pending visa applications, including questions about cases pending in administrative processing (attached).

3. A detailed description of the functions of the office responsible for administrative processing of SAOs:

   The Office of Screening, Analysis, and Coordination in the Visa Services Directorate (VO/SAC) is the primary interlocutor for the Bureau of Consular Affairs (CA) with other U.S. agencies involved in the national security screening of foreign travelers. It provides guidance to the field on security issues as they concern visa issuance and denial, primarily within the purview of INA Sections 212(a)(3) and 212(f), and exercises the Secretary of State's authority in recommending to the Secretary of Homeland Security waivers of ineligibility to permit such foreign nationals temporary admission to the United States.

   VO/SAC responds to all Security Advisory Opinion (SAO) requests submitted by consular officers adjudicating visa applications overseas. VO/SAC coordinates responses to SAO requests with law enforcement and intelligence agencies, other State Department bureaus and offices, as appropriate, and other U.S. government partners on visa matters involving national security, technology transfer, counterintelligence, human rights violations, and U.S. sanctions. VO/SAC also prudentially revokes visas as warranted, exercising the Secretary of State's authority under INA section 221(i), as warranted, and coordinates the Visas Viper program, which involves reports from overseas posts nominating individuals for entry into the Terrorist Identities Datamart Environment (TIDE), which is

managed by the National Counterterrorism Center, for onward movement to the Terrorist Screening Center (TSC) for inclusion in the Terrorist Screening Database (TSDB), when certain standards are met. The office also provides guidance and recommendations on visa policy related to national security exclusions, and represents CA on U.S. government steering groups related to screening, tracking, and watch-listing.

4. The total number of SAOs for years 2012 – 2017:

2012: 313,603
2013: 265,844
2014: 179,167
2015: 181,649
2016: 196,887
2017: 34,681 SAOs are currently open as of June 28, 2017.

5. A detailed description of the functions of the office responsible for coordinating and issuing SAOs:

See description at item 3, above.

6. As to whether information on administrative processing is reported, and if so to whom:

Neither VO/SAC nor any other entity within the Department reports on SAO processing for any purpose.

7. Any outcomes goals, quotas or requirements relating to administrative processing and/or SAO:

The goal of SAOs is to ensure visa decisions are informed by all relevant information available to the US government. There are no quotas. There are Department and broader US government requirements for when a consular officer must or may request an SAO; however, those are law enforcement sensitive.

8. A report reflecting SAOs broken down by nationality of visa applicant for each year 2012 – 2016:

See attached Excel spreadsheet with data tabs for all five years. Please note that these numbers are approximate as they were collated from multiple systems and there may be slight deviations from one system to another (attached).

9. A report we create for this purpose reflecting SAOs broken down by visa classification for each year 2012 – 2016:

   See attached Excel spreadsheet with data tabs for all five years. Please note that these numbers are approximate as they were collated from multiple systems and there may be slight deviations from one system to another (attached).

10. A report showing the percentage of SAOs closed within 60 days for each of the years 2012-2016:

   CY 2012 – 81%
   CY 2013 - 69%
   CY 2014 – 74%
   CY 2015 – 84%
   CY 2016 – 85%

   Please note that these numbers are approximate as they were collated from multiple systems and there may be slight deviations from one system to another.

11. The number of visas denied under section 212(a)(3)(B) for each of the years 2012 – 2016:

Refused 3B and Refused 3B/Waived

	2012	**2013**	**2014**	**2015**	**2016**
3B Refusals*	381	137	187	593	779
3B Refusals with Waivers**	533	428	482	422	325

**Dec previous year – Nov current year*
***Apr current year - Mar following year*

12. A statement on whether an SAO is required before a visa may be denied under INA section 212(a)(3)(B):

   State Department guidance requires an SAO before a visa may be denied on terrorism-related grounds.

The Department has now completed the processing of your request. If you have any questions you may write to the Office of Information Programs and Services, SA-2, Department of State, Washington DC 20522-8100, or contact the Office of Information Programs and Services by telephone at (202) 261-8484. Please be sure to refer to the case control number shown above in all correspondence about this case. Also, if you need any further assistance or would like to discuss any aspect of your request, please do not hesitate to contact our FOIA Public Liaison, email at FOIAProgram-DL@state.gov or telephone at 202-663-2222.

Sincerely,

for Chloe Dybdahl, Chief
Advisory Opinions Division
Directorate for Visa Services

Enclosures:

List of Attachments:

1. May 3, 2017 Congressional Testimony, House Committee on Homeland Security, DAS Ramotowski,
2. March 15, 2017 Congressional Testimony, Senate Judiciary Committee, AAS Donahue,
3. March 15, 2016 Congressional Testimony, Senate Homeland Security and Governmental Affairs Committee, PDAS Donahue,
4. February 3, 2016 Congressional Testimony, House Homeland Security Committee, AS Bond,
5. December 17, 2015 Congressional Testimony, Committee on House Oversight and Government Reform, AS Bond,
6. Department contact information for various visa situations, and
7. Excel spreadsheet of numbers of SAOs by visa category and nationality for years 2012-2016.

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.

DEPARTMENT OF STATE

WRITTEN TESTIMONY

OF

EDWARD J RAMOTOWSKI

DEPUTY ASSISTANT SECRETARY OF STATE

BUREAU OF CONSULAR AFFAIRS

DEPARTMENT OF STATE

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY

MAY 3, 2017

Good morning Chairman McCaul, Ranking Member Thompson, and distinguished Members of the Committee, and thank you for this opportunity to testify at today's hearing. The Department of State is fully 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. We are the first line of defense in border security, as the Department of State is often the first U.S. government agency to have contact with foreign nationals wishing to travel to the United States, and we fully share your commitment to preventing individuals from exploiting the visa process as a means of entering our country with the intent to do harm.

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, recent terror incidents both overseas and at home have 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 and public safety decision. The rigorous security screening regimen I describe below applies to all visa categories.

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 –including all applicants for which there are any concerns – 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 including those related to criminal history, prior visa applications or travel to the United States, and/or links to terrorism and other security threats.

Consular officers also employ a variety of statutory tools to adjudicate visa applications. Under the law that applies to most nonimmigrant visa classifications, if the consular officer believes a nonimmigrant visa applicant may fail to abide by the requirements of the visa category in question, the application will be refused under section 214(b) of the Immigration and Nationality Act (INA). A consular officer may also initially refuse a case under INA section 221(g) to confirm information presented in the application, request additional information from the applicant, request a security or legal review from Washington, or pursue local leads or other information to determine whether the applicant is subject to a security or non-security-related ineligibility. In FY 2016, consular officers denied 2,980,271 visas (includes both final and administrative refusals), conducted 138,324 fraud case reviews, and sent 36,258 requests for reconsideration to USCIS for petitions previously approved.

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 is populated, in part, through an export of the Terrorist Screening Database (TSDB), the federal terrorism watchlist. 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 internal 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 is a database 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. While the precise details of KFE vetting cannot be detailed in this document, 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 suspends the 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 or when otherwise required by interagency policy, 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. 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 29 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 can 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.

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 which are supplemented by computerized self-study tutorials to review this information. Adjudicators receive extensive classroom instruction on immigration law, Department policy and guidance, and consular systems, including how to review 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 participating in other in-class activities. Basic interviewing training includes instruction in techniques for questioning an applicant to elicit information relevant to assessing visa eligibility. Officers practice analyzing 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 Viper reporting program. Following the December 25, 2009 attempted terrorist attack on Northwest Flight 253, we strengthened the procedures and content requirements for Viper reporting. Chiefs of Mission are responsible for ensuring that all appropriate agencies and offices at post contribute relevant information for Viper nominations. 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 INA section 214(b), 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, the National Counterterrorism Center (NCTC), FBI, DHS/ICE, and DHS/CBP's National Targeting Center (NTC). All records added to the TSDB and Terrorist Identities Datamart Environment (TIDE) are checked against the CCD to determine if there are matching visa records. In addition to recurrently vetting against 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 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 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 screening, CBP uses these 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 an aircraft. 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. Since 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 in which 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 millions of visa applications we refuse each year, since 2001, the Department has revoked approximately 160,000 visas, based on information that surfaced following visa issuance, for a variety of reasons. This includes nearly 11,000 visas prudentially revoked after information emerged post-issuance suggesting possible 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. 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.

Executive Order 13780 on Protecting the Nation from Foreign Terrorist Entry into the United States (E.O.) signed by the President on March 6, 2017, and the Presidential Memorandum on Heightened Screening, articulate the Administration's commitment to rigorously enforce our immigration laws and continuously upgrade and refine our screening and vetting processes to keep the people of the United States safe. These actions range from interagency efforts to harmonize screening and vetting standards across multiple immigration programs to focusing on ways to improve our abilities to deport criminal aliens. Additionally, the Department recently instructed posts globally to develop criteria for identifying sets of visa applicant populations warranting increased scrutiny. We have likewise heightened vetting for any visa applicant that was ever present in ISIS-controlled territory, for example. In addition, we are working with the Departments of Homeland Security and Justice to implement these steps in compliance with all relevant court orders.

We are taking several measures to confront developing threats and respond to recent terrorist incidents both overseas and in the United States.

We constantly analyze our current processes, including security vetting, to identify areas where we could improve. We are working closely with DHS and the interagency to explore and analyze the use of social media screening of visa applicants. At the same time, we continue to explore methods and tools that 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, beginning in 2011 the Departments of State and Homeland Security 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, 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 on issues addressing our national security in a cooperative and productive manner.

Visa Waiver Program

The Visa Waiver Program (VWP) was established as a pilot program in 1986 to more efficiently use U.S. government resources. Since then, it has been steadily strengthened. The program enables nationals of 38 participating countries to travel to the United States for tourism or business stays of 90 days or less without obtaining a visa but subject to vetting through the Electronic System for Travel Authorization (ESTA) that is equivalent to the checks done when issuing a visa. Approximately 20 million people enter the United States each year under this program, enabling the Department of State to focus more resources on visa

applicants from countries that do not meet VWP's high security standards. The VWP enables the Department of State to focus more resources on visa applicants who merit additional scrutiny. It also allows us to benefit from information-sharing with VWP countries.

All travelers coming to the United States under the VWP undergo the same checks for ties to terrorism and are subject to the same multiple layers of security reviews as visa applicants, including fingerprint screening. While VWP travelers do not undergo a consular interview, they are required to provide certain biographic information for screening prior to travel through the Electronic System for Travel Authorization. Only citizens of VWP countries with an ESTA approved by DHS can travel to the United States under this program. Refugees, asylum seekers, and non-citizen residents of VWP countries cannot travel under VWP. The Department of State annually publishes the visitor visa refusal rates for every country. This information garners significant interest from countries aspiring to join VWP, as the refusal rate is the most visible of the VWP requirements.

Members of the Visa Waiver Program are our closest and most essential partners on counterterrorism. They are currently Andorra, Australia, Austria, Belgium, Brunei, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Taiwan, and the United Kingdom.

Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015

Under the *Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015*, nationals of VWP countries who are also nationals of Iran, Iraq, Sudan, or Syria, or have traveled to or been present in Iran, Iraq, Sudan, Syria, Libya, Yemen, or Somalia on or after March 1, 2011 are no longer eligible for VWP travel and require a visa to travel to the United States.

Those nationals who travelled to these countries for official or military service on behalf of a VWP country are statutorily exempt from the new requirement. Also, under the new Act, the Secretary of Homeland Security may

waive these travel-related VWP restrictions if he determines that such a waiver is in the law enforcement or national security interests of the United States. Such waivers are granted only on a case-by-case basis. In FY16, the Secretary of Homeland Security approved 211 such waivers.

Visa applications have increased by approximately eight percent in Visa Waiver Program countries since these legislative changes took effect in early 2016. Our data indicate that through December 2016, we facilitated visa services for 60,000 travelers affected by them. For example, for those who need a U.S. visa for urgent business, medical, or humanitarian travel to the United States, U.S. embassies and consulates provide visa interview appointments on an expedited basis.

DEPARTMENT OF STATE

WRITTEN TESTIMONY

OF

DAVID T. DONAHUE

ACTING ASSISTANT SECRETARY OF STATE

BUREAU OF CONSULAR AFFAIRS

DEPARTMENT OF STATE

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

ON

MARRIAGE FRAUD

MARCH 15, 2017

10:00 A.M.

226 DIRKSEN SENATE OFFICE BUILDING

WASHINGTON, D.C.

Good morning Chairman Grassley, Ranking Member Feinstein, and distinguished members of the Committee, thank you for the opportunity to testify at today's hearing. The Department of State (the "Department") is fully dedicated to protecting our nation's borders and has no higher priority than the safety of our fellow citizens at home and abroad. We are the first line of defense in border security because the Department is often the first U.S. government agency to have contact with foreign nationals wishing to travel to the United States. We fully share your commitment to preventing individuals who intend to do our nation harm from exploiting the K-1 fiancé or any other visa category as a means of entering our country, and I am pleased to share with you the robust fraud-prevention measures we have in place to prevent such an occurrence. These fraud prevention measures complement the multi-faceted security screening process we and our partner agencies have built to screen all visa applicants, including K-1 fiancés, well before any potential threat reaches our borders.

An Overview of the Marriage-Based Visa Process

The Department of State's role in the marriage-based visa process begins when our National Visa Center (NVC) receives an approved I-129F petition for a K-1 fiancé, or an I-130 petition for a spouse, directly from U.S. Citizenship and Immigration Services (USCIS). USCIS includes any relevant information from their petition approval process with the petition. NVC conducts a review of each petition received and prepares the visa case for adjudication by a consular official at a U.S. embassy or consulate. For every K-1 petition, NVC's Fraud Prevention Unit (FPU) conducts a review of potential fraud indicators. Should fraud indicators be found, the FPU will conduct a further, in-depth review using Department of State

records, commercial database checks, and internet checks of publically-available information. NVC's FPU summarizes the results of this review in a memo to the consular officer overseas who will ultimately determine whether or not the applicant qualifies for a visa. NVC also conducts additional, similar fraud reviews on targeted spousal visa petitions.

Once the visa case is documentarily complete at NVC, the applicant is scheduled for an interview with a consular officer overseas. Consular officers are trained in the language, culture, social and economic conditions, as well as security and fraud trends in their host country, and are provided with guidance in the Foreign Affairs Manual to apply U.S. immigration law appropriately. Understanding the cultural context surrounding engagement and marriage customs provides consular officers with key knowledge that can assist in making eligibility determinations. If required, the consular officer may request additional documentation or evidence of a relationship to assess the qualifications of the applicant for the visa category sought.

Most U.S. embassies and consulates have a Fraud Prevention Unit, headed by a Fraud Prevention Manager. If fraud is suspected, the visa application is sent to the FPU at post for further investigation. FPUs employ a number of technology tools and other methods to conduct fraud assessments, including referring cases for criminal investigation if necessary. More than 100 consular sections also integrate a Diplomatic Security special agent, a sworn federal law enforcement officer, detailed to the consular section, whose primary task is to conduct criminal investigations related to passport and visa fraud. These special agents coordinate criminal investigations and liaise with other U.S. and local law-enforcement agencies for any

consular-related issues, such as facilitating the arrest of visa vendors, assisting with law enforcement hits, and coordinating extraditions.

If a consular officer determines that the relationship claimed as the basis for the immigrant or fiancé visa petition is fraudulent, and exists solely to confer an immigration benefit to the visa applicant, the consular officer will return the petition to USCIS for reconsideration and possible revocation, as USCIS has the authority to make determinations regarding visa petitions. If USCIS reaffirms the petition, the consular officer will review the case and all new information and evidence contained in the file. Barring other ineligibilities or newly identified facts, the consular officer will generally issue the visa.

Consular Officer Training to Detect Fraud in Visa Applications

The Department of State trains all consular officers to recognize fraud indicators they may encounter while adjudicating visas. In addition to a mandatory six-week Basic Consular Course for all incoming consular officers, the Bureau of Consular Affairs and individual consular sections at U.S. embassies and consulates overseas provide ongoing training on regional visa fraud trends. The Office of Fraud Prevention Programs in Washington also offers multiple week-long in-person trainings on visa fraud prevention, and coordinates additional ongoing webinars for overseas Fraud Prevention Units, frequently conducted jointly with USCIS.

The Broader Security Screening Process

In coordination with interagency partners, the Department has developed, implemented, and refined an intensive visa application and screening process that is applied to all visa categories. 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, including K-1s.

All visa applicants submit online applications – K-1 applicants submit the DS-160 visa application form as they are considered nonimmigrants, and spouses of U.S. citizens and Lawful Permanent Residents submit the 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. During the interview, consular officers pursue case-relevant issues pertaining to the applicant's identity, qualifications for the particular visa category in question, prior visa applications or travel to the United States, and any information pertaining to possible ineligibilities, including ineligibilities related to criminal history, 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 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 going back to 1998. This robust searching capability, which takes into account variations in spelling, is central to our procedures.

We collect 10-print fingerprint scans from nearly all immigrant visa applicants, except , for those immigrant visa applicants 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 watchlist of available fingerprints of known and suspected terrorists, wanted persons, and immigration law violators; 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. 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 under 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 may suspend visa processing and request an SAO. Consular officers receive extensive training on the SAO process, which requires them to deny the visa application under the Immigration and Nationality Act (INA) section 221(g) , reflecting the consular officer does not have sufficient information to resolve potential ineligibilities, then submit the case for interagency review 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), DHS/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 high-threat posts of concern for DHS 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. When warranted, DHS officers assigned to VSUs conduct targeted, in-depth reviews of individual visa applications and applicants prior to issuance, and make recommendations to the consular officer regarding refusal of an application or revocation of an issued visa. This collaboration highlights how 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.

K Visa Data Analysis

In 2016, the Department of State partnered with USCIS to conduct a review of five years of data on K-1 visa recipients to determine if the visa holders complied with the terms of their visas and properly adjusted to lawful permanent resident status or

departed the United States at the end of the initial period of admission. Results showed the vast majority of K-1 recipients – approximately 98 percent – used their visas appropriately by adjusting status as a result of marriage, departing following entry (indicating they did not pursue the marriage), or adjusting through other lawful means.

Conclusion

Mr. Chairman, Ranking Member Feinstein, and distinguished Members of the Committee, the Department of State has no higher priority than the safety of our fellow citizens at home and overseas, and the security of the traveling public. We approach every visa adjudication with the interest of safety and security and work diligently to ensure that those attempting to commit visa fraud are caught at the time of the visa interview and future fraudulent applicants are deterred. We appreciate the support of Congress as we work to strengthen our defenses and continue our efforts to ensure that those applicants entitled to visas under U.S. laws are granted while those not entitled are stopped prior to attempting to enter the United States.

I look forward to your questions.

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.

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 HOMELAND SECURITY

HEARING

ON

CRISIS OF CONFIDENCE: PREVENTING TERRORIST INFILTRATION THROUGH U.S. REFUGEE AND VISA PROGRAMS

FEBRUARY 3, 2016

Good morning Chairman McCaul, Ranking Member Thompson, 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, 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 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. Lessons learned through the years have led to significant improvements in procedures and capabilities. At the same time, the tragic events that transpired most recently in San Bernardino demonstrated that no system is perfect. We must 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 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 found ineligible for visas, or regarding whom potentially derogatory information exists, 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 going back to 1998. This robust searching capability, which takes into account variations in spelling, 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 watchlist of available fingerprints of known and suspected terrorists, wanted persons, and immigration law violators; 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. 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, then 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, or with particular nationality, place of birth, or residence information. In any case in which reasonable grounds exist regardless of name check results, a consular officer may suspend visa processing and institute SAO procedures. Consular officers receive extensive training on the SAO process, which requires them to issue an interim denial of a visa application and engage in interagency review for any case with possible security ineligibilities. 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 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 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, the National Counterterrorism Center (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. Vetting partners sends 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, as well as 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.

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 law enforcement or immigration stakeholders. We are mindful, however, not to act unilaterally, but to coordinate expeditiously with our national security partners in order to avoid possibly disrupting 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.

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 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 processing of 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 could potentially 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 the President 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.

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.

State Department Contacts for Various Visa Questions.		
I am (immigrant/nonimmigrant) Visa applicant)	And looking to check on my U.S. Visa application status	Consular Electronic Application Center (CEAC)
I am an attorney or accredited representative	And my client's petitions is undergoing processing at the National Visa Center	Email: NVCattorney@state.gov
I have an approved immigrant visa petition from USCIS	And my petition has been sent to the National Visa Center (NVC) for visa pre-processing	National Visa Center (NVC) Phone (603) 334-0700 7:00 a.m. – 1200 a.m. EST Monday through Friday (excluding holidays)
I have an approved immigrant visa petition from USCIS	And the National Visa Center (NVC) has completed visa pre-processing and sent my case to the U.S. Embassy or Consulate.	National Visa Center (NVC) Phone (603) 334-0700 7:00 a.m. – 12:00 a.m. EST Monday through Friday (excluding Holidays)
I have been selected for a Diversity Visa	And my questions have not been answered on the E-DV website or the Diversity Visa Instructions	Kentucky Consular Center (KCC) Phone (606) 526-7500 7:30 a.m. – 4:00 a.m. EST Email. KCCDV@state.gov You must include your name, birthdate and case number exactly as they appear in the Entrant
I would like to apply for a nonimmigrant visa	And I have questions that have not been answered on this website or on the website of the U.S. Embassy or Consulate where I plan to apply	We recommend you review the information on travel.state.gov or contact, National Visa Center (NVC) Phone: (603) 334-0888 7:00 a.m. – 12:00 a.m. EST Monday through Friday (excluding holidays) The NVC is unable to answer nonimmigrant
I have a J-1 exchange visitor visa	And have questions about a waiver of the Two Year Home Country Foreign Residence	The Visa Office Email 212ewaiver@state.gov
I have a J-1 exchange visitor visa	And have questions about my pending application for a Waiver of the Two Year Home Country Foreign Residence Requirement.	The Visa Office Online: J waiver status Email: 212ewaiver@state.gov and include: the case number; the applicant's last name, first name, and date of birth; the

		basis for the waiver application, and; a brief explanation of your inquiry.
I am applying for a visa	And I am looking for my nearest U.S. Embassy or Consulate	Click on the link to locate your nearest U.S. Embassy or Consulate
I have OR my client has a pending visa application at an Embassy or Consulate	And the application is pending administrative processing. I have questions regarding the status of the application.	Contact the Embassy or Consulate Where the application is pending
I am an applicant or attorney	Legal questions about a specific case when an applicant or attorney has tried to contact post at least twice regarding the specific issue without receiving a final response, and where 30 days have passed since the second inquiry; Legal question about a specific case in which an applicant or attorney has received a final response from post, but believes it to be wrong as a matter of law (note this does not include review of INA 214(b) refusals); Legal questions about specific cases involving T visas U visas, Diversity visas, or adoption, cases; and Legal questions about specific cases involving the Child Status Protections Act (CSPA) or the Violence Against Women Act (VAWA)	LegalNet@state.gov

2012			
Visa Class	**SAOs**	**Nationality**	**SAOs**
A1	701	AFGH	4,969
A2	10,861	ALB	146
A3	150	ALGR	390
B1	1,751	ANGL	2
B1/B2	172,245	ANTI	6
B2	5,606	ARG	1,330
BBBCC	11,151	ARM	33
BBBCV	4,610	ASTL	326
BC3	1	AUST	42
C1	217	AZR	76
C1/D	6,102	BAHR	1,147
C2	5	BAMA	29
C3	155	BANG	9,479
C51	4	BELG	52
C52	1	BENN	45
CM1	7	BHU	5
CP1	287	BIH	49
CP2	1	BLZ	106
CP3	46	BOL	202
CP5	1	BOT	3
CR1	3,272	BRDO	7
CR2	58	BRND	19
CW1	10	BRNI	106
CW2	1	BRZL	4,070
D	250	BULG	55
DV1	1,620	BURK	23
DV2	684	BURM	538
DV3	53	BYS	354
E1	157	CAFR	9
E11	46	CAN	511
E13	5	CAVI	19
E14	30	CAYI	4
E15	3	CBDA	3
E2	255	CHAD	161
E21	55	CHIL	856
E22	27	CHIN	52,944
E23	6	CMRN	33
E3	45	COD	40
E31	123	COL	5,674
E32	15	COMO	43
E34	57	CONB	6
E35	67	CSTR	960
E3D	6	CUBA	2,321
E3R	3	CYPR	29
EW3	27	CZEC	6
EW4	11	DEN	55
EW5	9	DJI	434

F1	24,855	DOMN	16
F11	649	DOMR	1,792
F12	79	ECUA	1,368
F2	911	EGN	2
F21	707	EGYP	8,575
F22	648	ELSL	2,504
F23	48	ERI	133
F24	537	EST	5
F25	38	ETH	643
F2A	24	FIJI	67
F2B	8	FIN	12
F3	11	FRAN	371
F31	496	GABN	12
F32	479	GAM	91
F33	442	GEO	20
F4	16	GER	503
F41	2,893	GHAN	445
F42	2,221	GNEA	217
F43	2,045	GRBR	1,300
FX	5	GRC	29
FX1	512	GREN	16
FX2	496	GUAT	273
FX3	54	GUIB	3
G1	596	GUY	1,277
G2	1,531	HAT	54
G3	33	HNK	337
G4	1,005	HOKO	31
G5	16	HOND	228
H1B	7,796	HRV	32
H1B1	12	HUNG	13
H2A	730	ICLD	1
H2B	514	IDSA	3,843
H3	280	IND	30,709
H4	1,034	IRAN	18,207
I	287	IRAQ	10,556
I5	3	IRE	103
I51	238	ISRL	6,184
I52	166	ITLY	86
I53	12	IVCO	76
IB2	4	JAM	134
IB3	7	JORD	4,306
IR1	2,825	JPN	42
IR2	1,174	JRSM	1
IR3	2	KAZ	27
IR4	8	KENY	331
IR5	6,740	KGZ	10
IW	1	KIRI	1
IW1	9	KOR	36
IW2	3	KSV	109

J1	14,924	KUWT	4,918
J2	921	LATV	25
K1	1,070	LBYA	1,050
K2	3	LEBN	3,191
K3	38	LIBR	35
K4	8	LITH	3
L1	2,572	LXM	2
L2	491	MAC	16
LPR	22	MADG	26
M1	460	MALI	199
M2	1	MALW	22
N8	1	MAUR	405
NATO2	32	MEX	21,118
NATO4	4	MKD	39
NATO5	1	MLAS	1,738
NATO6	1	MLD	8
O1	196	MLDV	180
O2	68	MLTA	2
O3	13	MONG	1
P1	253	MORO	2,655
P3	241	MOZ	4
P4	3	MRTS	24
Q1	13	MTG	9
R1	69	NAU	1
R2	13	NEP	354
SB1	37	NETH	92
SD1	6	NIC	184
SD2	1	NIR	61
SD3	2	NORW	66
SE	1	NRA	2,057
SE1	51	NZLD	36
SE2	9	OMAN	350
SE3	46	PAL	1,684
SI1	175	PAN	181
SI2	79	PARA	146
SI3	10	PERU	1,604
SK1	1	PHIL	1,544
SQ	7	PKST	31,153
SQ1	3,343	POL	37
SQ2	1,551	PORT	35
SQ3	386	PRK	73
SR1	5	QTAR	247
SR2	1	ROM	63
SR3	1	RUS	10,605
SU3	1	RWND	97
T2	5	SAFR	439
T3	2	SARB	18,088
TD	42	SBA	100
TN	140	SENG	256

U1	4
U2	2
U3	8
U4	1
YY	76
ZZ	64
(blank)	119
Grand Total	311,591

SEYC	4
SING	439
SLCA	10
SLEO	100
SOMA	667
SPN	709
SRL	577
SSDN	10
STCN	57
STPR	1
STVN	2
SUDA	1,215
SURM	18
SVK	6
SVN	3
SWDN	152
SWTZ	81
SYR	1,818
TAZN	235
TCIS	2
THAI	21
TJK	5
TKM	12
TMOR	3
TNSA	572
TOGO	19
TONG	1
TRIN	708
TRKY	2,841
TWAN	2,175
UAE	2,773
UGAN	20
UKR	1,125
UNLP	14
URU	106
UZB	56
VANU	2
VENZ	3,326
VTNM	71
XWB	3
XXX	469
YEM	2,965
ZAMB	6
ZIMB	56
(blank)	65
Grand Total	311,591

2013			
Visa Class	**SAOs**	**Nationality**	**SAOs**
A1	908	MON	1
A2	11,432	AFGH	8,423
A3	186	ALB	123
B1	1,993	ALGR	505
B1/B2	150,232	ANGL	18
B2	7,466	ANTI	8
BBBCC	4,879	ARG	644
BBBCV	94	ARM	26
BC1	4	ASTL	309
BC2	1	AUST	29
BC3	1	AZR	80
C1	137	BAHR	824
C1/D	3,439	BAMA	8
C2	3	BANG	8,418
C3	80	BELG	64
C51	1	BENN	25
CM1	3	BERM	1
CP1	109	BHU	5
CP2	1	BIH	46
CP3	6	BLZ	61
CP5	1	BOL	121
CR1	2,092	BOT	1
CR2	25	BRDO	15
CW1	19	BRND	33
CW2	8	BRNI	25
D	232	BRZL	2,662
DV1	2,171	BULG	123
DV2	996	BURK	9
DV3	56	BURM	481
E1	162	BYS	324
E11	69	CAFR	3
E12	1	CAN	365
E13	8	CAVI	21
E14	25	CAYI	2
E15	12	CBDA	3
E2	181	CHAD	128
E21	62	CHIL	361
E22	27	CHIN	59,398
E23	6	CMRN	20
E3	50	COD	43
E31	102	COL	4,617
E32	3	COMO	31
E34	43	CONB	10
E35	30	CSTR	244
E3D	12	CUBA	2,316
E3R	6	CYPR	22
EW3	10	CZEC	8

EW4	4	DEN	41
EW5	7	DJI	182
EX1	1	DOMN	19
F1	22,989	DOMR	573
F11	515	ECUA	1,004
F12	60	EGN	1
F2	898	EGYP	8,422
F21	417	ELSL	962
F22	198	ERI	108
F23	25	EST	5
F24	382	ETH	432
F25	7	FIJI	55
F2A	6	FIN	11
F2B	6	FRAN	457
F3	1	GABN	9
F31	301	GAM	50
F32	324	GEO	40
F33	242	GER	420
F4	7	GHAN	237
F41	1,441	GNEA	261
F42	1,101	GRBR	670
F43	923	GRC	47
FX	6	GREN	12
FX1	609	GUAT	205
FX2	368	GUIB	8
FX3	21	GUY	427
G1	567	HAT	150
G2	1,259	HNK	407
G3	29	HOKO	22
G4	856	HOND	389
G5	6	HRV	61
H1B	5,611	HUNG	13
H1B1	6	IDSA	2,424
H2A	468	IND	21,239
H2B	565	IOT	1
H3	134	IRAN	21,969
H4	646	IRAQ	9,445
I	191	IRE	129
I51	151	ISRL	5,393
I52	103	ITLY	92
I53	12	IVCO	91
IB1	3	JAM	51
IB3	1	JORD	2,804
IR1	1,834	JPN	33
IR2	692	JRSM	3
IR4	6	KAZ	41
IR5	4,039	KENY	256
IW1	6	KGZ	7
J1	14,567	KOR	61

J2	960	KSV	73
K1	763	KUWT	4,378
K2	3	LAOS	2
K3	25	LATV	19
K4	6	LBYA	1,667
L1	2,007	LCHT	1
L2	273	LEBN	2,434
LPR	22	LIBR	60
M1	480	LITH	1
M2	4	MAC	18
NATO1	1	MADG	25
NATO2	27	MALI	192
NATO6	1	MALW	12
O1	169	MAUR	518
O2	22	MEX	10,073
O3	16	MKD	31
P1	150	MLAS	546
P3	149	MLD	7
P4	2	MLDV	109
Q1	6	MLTA	6
R1	53	MONG	3
R2	7	MORO	1,460
SB1	42	MOZ	3
SD3	4	MRTS	5
SE	1	MTG	25
SE1	40	NEP	448
SE2	7	NETH	50
SE3	32	NIC	112
SI1	59	NIR	50
SI2	62	NORW	43
SI3	20	NRA	1,683
SQ	6	NZLD	25
SQ1	4,701	OMAN	151
SQ2	2,849	PAL	1,217
SQ3	545	PAN	135
SR1	1	PARA	110
SR2	1	PERU	670
T3	1	PHIL	382
TD	26	PKST	19,054
TN	70	POL	49
U1	2	PORT	25
U2	1	PRK	59
U3	5	QTAR	1,538
U4	2	ROM	50
V1	1	RUS	9,337
V2	1	RWND	61
YY	59	SAFR	290
ZZ	53	SARB	17,416
(blank)	99	SBA	80

Grand Total	263,831

SENG	292
SEYC	1
SING	171
SLCA	10
SLEO	71
SNTD	2
SOMA	688
SPN	337
SRL	286
SSDN	113
STCN	110
STVN	3
SUDA	1,343
SURM	12
SVK	2
SVN	1
SWDN	100
SWTZ	78
SYR	1,558
TAZN	198
THAI	11
TJK	9
TKM	4
TNSA	419
TOGO	8
TONG	3
TRIN	237
TRKY	2,139
TWAN	551
UAE	1,511
UGAN	28
UKR	1,162
UNLP	4
URU	35
UZB	81
VENZ	3,693
VTNM	238
XGZ	1
XWB	2
XXX	282
YEM	2,522
ZAMB	7
ZIMB	28
(blank)	34
Grand Total	263,831

2014			
Visa Class	**SAOs**	**Nationality**	**SAOs**
A1	615	AFGH	5,168
A2	6,393	ALB	16
A3	94	ALGR	219
B1	1,093	ANGL	2
B1/B2	108,501	ANTI	4
B2	2,655	ARG	61
BBBCC	487	ARM	33
BBBCV	23	ASTL	219
BC1	1	AUST	16
C1	89	AZR	92
C1/D	811	BAHR	391
C2	3	BAMA	1
C3	39	BANG	3,310
CM1	1	BELG	44
CP1	71	BENN	5
CP3	3	BHU	3
CR1	549	BIH	38
CR2	4	BLZ	6
CW1	4	BOL	29
CW2	6	BRDO	3
D	79	BRND	26
DV1	1,183	BRZL	452
DV2	658	BULG	42
DV3	12	BURK	11
E1	176	BURM	200
E11	78	BYS	360
E12	1	CAFR	4
E13	3	CAN	231
E14	37	CAVI	1
E2	107	CBDA	2
E21	53	CHAD	85
E22	23	CHIL	35
E23	1	CHIN	57,519
E3	53	CMRN	10
E31	71	COD	37
E32	7	COL	2,580
E34	30	COMO	7
E35	18	CONB	6
E3D	13	CSTR	93
E3R	5	CUBA	2,367
EW3	7	CYPR	5
EW4	4	CZEC	5
EW5	1	DEN	16
F1	18,325	DJI	41
F11	243	DOMN	18
F12	10	DOMR	67
F2	688	ECUA	168

F21	246	EGYP	4,219
F22	62	ELSL	64
F23	4	ERI	28
F24	145	ETH	31
F2A	1	FIJI	21
F3	1	FIN	10
F31	176	FRAN	215
F32	207	GABN	2
F33	80	GAM	20
F4	3	GEO	19
F41	741	GER	241
F42	518	GHAN	30
F43	351	GNEA	277
FX1	219	GRBR	396
FX2	90	GRC	36
FX3	7	GREN	6
G1	393	GUAT	44
G2	1,096	GUIB	3
G3	39	GUY	24
G4	500	HAT	209
G5	4	HNK	385
H1B	4,175	HOKO	26
H1B1	5	HOND	30
H2A	41	HRV	37
H2B	14	HUNG	8
H3	55	IDSA	468
H4	409	IND	13,783
I	96	IRAN	21,764
I5	1	IRAQ	5,524
I51	117	IRE	116
I52	96	ISRL	5,366
I53	2	ITLY	65
IB3	1	IVCO	45
IR1	715	JAM	20
IR2	217	JORD	1,513
IR5	1,773	JPN	69
IW1	4	KAZ	20
IW2	1	KENY	119
J1	12,672	KGZ	16
J2	815	KOR	57
K1	597	KSV	51
K2	2	KUWT	2,483
K3	8	LAOS	1
L1	1,396	LATV	3
L2	169	LBYA	749
LPR	17	LEBN	1,128
M1	214	LIBR	134
N8	2	LITH	3
NATO2	21	LXM	1

NATO4	1
O1	159
O2	7
O3	15
P1	39
P2	1
P3	66
PARCIS	6
Q1	2
R1	14
R2	3
SB1	25
SD2	1
SE1	15
SE2	5
SE3	13
SI	1
SI1	71
SI2	14
SI3	8
SQ	4
SQ1	3,066
SQ2	1,346
SQ3	235
T2	1
T51	1
TD	13
TN	12
U3	4
YY	28
ZZ	53
(blank)	78
Grand Total	177,153

MAC	18
MADG	7
MALI	82
MALW	1
MAUR	523
MEX	674
MKD	11
MLAS	449
MLD	5
MLDV	8
MLTA	1
MONG	3
MORO	159
MOZ	5
MRTS	4
MTG	17
NEP	245
NETH	65
NIC	25
NIR	25
NORW	29
NRA	393
NZLD	12
OMAN	130
PAL	550
PAN	156
PARA	29
PERU	207
PHIL	80
PKST	10,300
POL	46
PORT	15
PRK	65
QTAR	1,545
ROM	21
RUS	6,967
RWND	91
SAFR	75
SARB	10,058
SBA	33
SENG	299
SING	56
SLCA	1
SLEO	178
SOMA	436
SPN	80
SRL	34
SSDN	117
STCN	109

SUDA	867
SURM	10
SVK	3
SWDN	73
SWTZ	36
SYR	833
SZLD	1
TAZN	34
THAI	23
TJK	6
TKM	2
TMOR	1
TNSA	137
TOGO	7
TRIN	23
TRKY	799
TWAN	630
UAE	1,111
UGAN	21
UKR	987
UNLP	15
URU	7
UZB	53
VENZ	600
VTNM	633
WSAM	4
XXX	115
YEM	1,702
ZAMB	8
ZIMB	40
(blank)	6
Grand Total	177,153

2015			
Visa Class	**SAOs**	**Nationality**	**SAOs**
A1	580	AFGH	7,219
A2	5,183	ALB	17
A3	44	ALGR	282
B1	1,047	ANGL	2
B1/B2	110,896	ANTI	3
B2	1,370	ARG	48
BBBCC	512	ARM	50
BBBCV	16	ASTL	239
BC1	2	AUST	18
BC2	1	AZR	152
BC3	1	BAHR	586
C1	67	BAMA	3
C1/D	799	BANG	1,987
C2	8	BELG	48
C21	1	BENN	11
C3	50	BHU	1
CF3	3	BIH	41
CP1	90	BLZ	10
CP2	1	BOL	30
CPD	35	BOT	2
CR1	627	BRDO	5
CR2	3	BRND	30
CW1	11	BRNI	2
D	94	BRZL	556
DV1	1,309	BULG	49
DV2	743	BURK	23
DV3	4	BURM	119
E1	110	BYS	346
E11	116	CAN	261
E12	1	CAVI	1
E13	4	CBDA	2
E14	47	CHAD	239
E15	2	CHIL	19
E2	103	CHIN	66,445
E21	70	CMRN	10
E22	25	COD	22
E3	56	COL	2,412
E31	22	COMO	20
E32	2	CONB	4
E34	13	CSTR	80
E35	3	CUBA	3,005
E3D	10	CYPR	8
E3R	7	CZEC	3
EW3	4	DEN	37
EW4	1	DJI	47
F1	18,388	DOMN	20
F11	183	DOMR	69

F12	4	ECUA	129
F2	594	EGN	1
F21	110	EGYP	3,369
F22	42	ELSL	41
F23	3	ERI	41
F24	169	EST	5
F2A	2	ETH	54
F2B	1	FIJI	25
F3	5	FIN	13
F31	142	FRAN	195
F32	183	GABN	8
F33	61	GAM	71
F4	2	GEO	24
F41	496	GER	290
F42	391	GHAN	28
F43	119	GNEA	360
FX1	205	GRBR	414
FX2	84	GRC	39
FX3	14	GREN	5
G1	382	GUAT	46
G2	1,272	GUIB	5
G3	44	GUY	21
G4	469	HAT	61
G5	2	HNK	434
H1B	4,120	HOKO	25
H1B1	4	HOND	39
H2A	51	HRV	46
H2B	53	HUNG	18
H3	57	IDSA	415
H4	450	IND	14,016
I	107	IRAN	20,901
I51	103	IRAQ	4,744
I52	92	IRE	107
I53	5	ISRL	3,855
IR1	711	ITLY	69
IR2	168	IVCO	69
IR3	1	JAM	32
IR5	1,694	JORD	2,403
IW1	3	JPN	119
IW2	3	KAZ	32
J1	12,428	KENY	159
J2	777	KGZ	27
K1	436	KOR	107
K2	2	KSV	118
K3	7	KUWT	1,451
K4	6	LATV	3
L1	1,552	LBYA	433
L2	185	LEBN	1,049
LPR	21	LIBR	364

M1	128
M2	1
NATO2	12
NATO4	2
NATO6	4
O1	248
O2	10
O3	23
P1	63
P2	1
P3	45
PARCIS	6
Q1	2
R1	15
R2	1
SB1	23
SD1	1
SD2	1
SD3	1
SE1	4
SE2	7
SE3	4
SI1	62
SI2	22
SI3	15
SQ	14
SQ1	5,209
SQ2	2,470
SQ3	374
T51	1
T52	1
TD	18
TN	15
U2	1
U4	1
YY	83
ZZ	181
(blank)	69
Grand Total	179,634

LITH	4
LXM	2
MAC	16
MADG	12
MALI	100
MALW	2
MAUR	423
MEX	704
MKD	22
MLAS	713
MLD	2
MLDV	12
MLTA	1
MONG	3
MORO	128
MOZ	10
MRTS	1
MTG	12
NEP	304
NETH	67
NIC	20
NIR	63
NORW	26
NRA	424
NZLD	7
OMAN	253
PAL	714
PAN	78
PARA	29
PERU	217
PHIL	134
PKST	8,600
POL	65
PORT	19
PRK	124
QTAR	1,156
ROM	70
RUS	7,446
RWND	89
SAFR	84
SARB	6,405
SBA	51
SENG	438
SEYC	2
SING	42
SLCA	2
SLEO	238
SOMA	302
SPN	68

SRL	38
SSDN	60
STCN	97
STPR	2
SUDA	742
SURM	10
SVK	2
SWDN	126
SWTZ	40
SYR	854
TAZN	35
THAI	12
TJK	15
TKM	1
TMOR	1
TNSA	99
TOGO	4
TRIN	66
TRKY	1,692
TWAN	823
UAE	1,194
UGAN	21
UKR	999
UNLP	4
URU	14
UZB	94
VAT	1
VENZ	532
VTNM	475
XXX	70
YEM	881
ZAMB	10
ZIMB	37
(blank)	16
Grand Total	179,634

2016			
Visa Class	**SAOs**	**Nationality**	**SAOs**
A1	536	AFGH	4,527
A2	5,794	ALB	24
A3	86	ALGR	246
B1	1,361	ANGL	3
B1/B2	124,035	ANTI	5
B2	1,122	ARG	54
BBBCC	423	ARM	75
BBBCV	21	ASTL	580
BC1	2	AUST	102
BC2	2	AZR	256
C1	82	BAHR	779
C1/D	1,575	BAMA	2
C3	48	BANG	2,375
C51	1	BELG	104
CM1	4	BENN	18
CP1	69	BERM	1
CPD	32	BHU	1
CR1	750	BIH	77
CR2	7	BLZ	4
CW1	50	BOL	36
D	84	BRDO	11
DV1	1,363	BRND	15
DV2	723	BRNI	1
DV3	11	BRZL	480
E1	375	BULG	102
E11	171	BURK	40
E12	1	BURM	144
E13	2	BYS	343
E14	64	CAFR	1
E15	3	CAN	300
E2	125	CAVI	3
E21	148	CAYI	2
E22	60	CBDA	3
E23	2	CHAD	328
E3	36	CHIL	17
E31	19	CHIN	73,858
E32	3	CMRN	3
E34	17	COD	19
E35	3	COL	3,150
E3D	11	COMO	6
E3R	7	CONB	6
EW	1	CSTR	53
EW3	69	CUBA	2,636
EW4	31	CYPR	21
EW5	1	CZEC	11
F1	17,092	DEN	115
F11	323	DJI	66

F12	5	DOMN	35
F2	564	DOMR	94
F21	186	ECUA	141
F22	39	EGN	3
F23	4	EGYP	3,773
F24	212	ELSL	50
F25	2	ERI	158
F2A	2	EST	3
F2B	1	ETH	144
F31	183	FIJI	17
F32	174	FIN	50
F33	63	FRAN	366
F4	1	FSM	1
F41	653	GABN	4
F42	447	GAM	84
F43	185	GEO	25
FX	1	GER	1,044
FX1	330	GHAN	60
FX2	127	GNEA	830
FX3	27	GRBR	1,253
G1	423	GRC	42
G2	1,219	GREN	9
G3	53	GUAT	31
G4	487	GUIB	7
G5	2	GUY	30
H1B	4,913	HAT	79
H1B1	2	HNK	492
H2A	56	HOKO	33
H2B	32	HOND	38
H3	63	HRV	22
H4	545	HUNG	33
I	119	ICLD	4
I5	1	IDSA	972
I51	89	IND	14,684
I52	77	IRAN	19,125
I53	9	IRAQ	5,040
IR1	856	IRE	113
IR2	304	ISRL	4,227
IR5	1,829	ITLY	205
IW	1	IVCO	86
IW1	3	JAM	35
IW2	3	JORD	2,715
J1	13,822	JPN	139
J2	854	KAZ	35
K1	554	KENY	228
K2	1	KGZ	21
K3	9	KOR	132
L1	1,515	KSV	167
L2	229	KUWT	1,567

LPR	32
M1	159
NATO2	25
NATO6	2
O1	269
O2	65
O3	29
P1	93
P3	68
PARCIS	18
Q1	2
R1	9
R2	1
SB1	21
SE1	5
SE2	7
SE3	1
SI	3
SI1	154
SI2	56
SI3	12
SQ	90
SQ1	3,251
SQ2	1,092
SQ3	376
T51	7
T52	4
T53	1
TD	11
TN	9
U3	1
YY	329
ZZ	590
(blank)	58
Grand Total	194,871

LATV	6
LBYA	375
LEBN	902
LIBR	850
LITH	8
LXM	9
MAC	18
MADG	1
MALI	143
MALW	2
MAUR	257
MEX	559
MKD	26
MLAS	762
MLD	6
MLDV	45
MLTA	2
MONG	6
MORO	200
MOZ	8
MRTS	2
MTG	35
NEP	395
NETH	229
NIC	39
NIR	75
NORW	109
NRA	455
NZLD	40
OMAN	246
PAL	728
PAN	89
PARA	16
PERU	194
PHIL	230
PKST	8,916
PNG	1
POL	65
PORT	40
PRK	77
QTAR	1,121
RMI	1
ROM	96
RUS	8,011
RWND	50
SAFR	84
SARB	6,476
SBA	88
SENG	619

SING	37
SLCA	2
SLEO	375
SNTD	10
SOMA	722
SPN	88
SRL	63
SSDN	43
STCN	109
STVN	2
SUDA	995
SURM	7
SVK	3
SVN	2
SWDN	446
SWTZ	137
SYR	812
TAZN	52
THAI	4
TJK	19
TKM	7
TNSA	143
TOGO	4
TONG	7
TRIN	46
TRKY	2,323
TWAN	1,267
UAE	1,245
UGAN	92
UKR	1,171
UNLP	1
URU	15
UZB	110
VANU	1
VENZ	391
VTNM	457
XXX	57
YEM	1,392
ZAMB	5
ZIMB	33
(blank)	15
Grand Total	194,871