NAVAL POSTGRADUATE SCHOOL CENTER FOR HOMELAND DEFENSE AND SECURITY
HOMELAND SECURITY DIGITAL LIBRARY
SECURING THE HOMELAND THROUGH THE POWER OF INFORMATION

MARCH 15, 2016

THE SECURITY OF U.S. VISA PROGRAMS

UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS

ONE HUNDRED FOURTEENTH CONGRESS, SECOND SESSION

HEARING CONTENTS:

MEMBER STATEMENTS

WITNESS STATEMENTS

AVAILABLE WEBCAST(S):*

[Watch Full Hearing]

This hearing compilation was prepared by the Homeland Security Digital Library,
Naval Postgraduate School, Center for Homeland Defense and Security.

COMPILED FROM:

- *http://www.hsgac.senate.gov/hearings/the-security-of-us-visa-programs*

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Chairman Johnson Opening Statement
"The Security of U.S. Visa Programs"

Tuesday, March 15, 2016

As submitted for the record:

Good morning. Thank you for joining us today.

Last December, the United States experienced the worst domestic terrorist attack since Sept. 11, 2001, when Syed Rizwan Farook and his wife, Tafsheen Malik, opened fire on an office holiday party in San Bernardino, Calif. — killing 14 and wounding 22.

Malik had immigrated to the United States legally from Saudi Arabia in 2014 on a fiancée visa, after reportedly meeting Farook on the Internet.

This horrific attack reminded us of the grave danger we face if we allow the wrong people to enter the country. It is a reminder of why the security of our visa program is so important.

In response to this attack, last year Congress and the Obama administration joined together to enact reforms to strengthen the Visa Waiver Program, through legislation that I and others sponsored.

Reforming the Visa Waiver Program represented a real improvement to our national security — requiring enhanced screening of foreign nationals who had traveled to certain countries like Iraq and Syria. But these improvements are premised on the integrity and security of the U.S. visa system and the traditional screening process.

With millions of people applying for visas to come to the United States, we face a daunting challenge: vetting the applications, screening and interviewing the foreign nationals, and, if they are granted a visa, ensuring that they follow the law and terms of their visas.

This is a challenge that dates back to 2001 and the Sept. 11 attacks. The bipartisan 9/11 Commission warned us that the al-Qaida hijackers defeated our immigration system, and that immigration security was critical for national security.

Now, 15 years later, the security of our immigration system is more critical than ever — particularly given the growth and spread of Islamic extremist terrorist organizations across the world and the rise in ISIS-inspired attacks on our own soil.

The purpose of our hearing this morning is to examine the state of visa security and to answer the following questions:

First, are we doing all that we can to screen and vet visa applicants before they enter the country?

Second, how effectively are federal agencies managing their responsibilities and working together — including sharing information — through each step of the visa and immigration process to ensure our security?

I am particularly interested to understand how the DHS components represented here today are working together — including overseeing key visa programs, sharing information, and preventing fraud and national security threats.

The American people are counting on us to keep them safe. That depends on the security and integrity of our immigration system. It requires the State Department and the Department of Homeland Security, as well as their components, to work effectively together as one team to protect us.

I am pleased that we have representatives from the State Department and the Department of Homeland Security with us today to address these serious questions.

You each have important jobs and responsibilities. I look forward to your testimony.

Statement of Ranking Member Tom Carper
"The Security of U.S. Visa Programs"

Tuesday, March 15, 2016

As prepared for delivery:

This hearing is the third in a series we have held to explore whether we are doing enough to address concerns that terrorists might try to exploit international travel to infiltrate our country.

In the aftermath of the Paris terrorist attacks, this Committee first scrutinized the process in place to screen and vet Syrian refugees escaping the carnage in the Middle East. We learned that the U.S. refugee resettlement process involves extensive security screening. Syrian refugees, we were told, undergo multiple rounds of screening over an average of 18 to 24 months, including in-person interviews by immigration analysts and counterterrorism officials trained in spotting fraud and deception.

The Committee next looked at our Visa Waiver program, which allows citizens of certain nations to travel to the United States for short visits without a visa. Once it became clear that the Paris terrorists held passports from European countries whose citizens enjoy visa waiver privileges, fears arose that this program could pose a security threat.

We learned that Visa Waiver travelers seeking to come to the United States endure nearly the same level of scrutiny and vetting as all other travelers. We also learned that when it comes to security, nothing is being 'waived', as the name of the program incorrectly suggests. And we learned that, in return for their entry into the Visa Waiver program, countries must share intelligence with the United States, they must open up their counter terrorism and aviation security systems to our inspectors, and they must abide by our standards for aviation and passport security.

As a result, the Visa Waiver program has now become a key counter terrorism tool.

Today we will continue this look at our screening systems for foreigners entering our country. We will examine the depth of security for all forms of visas, whether they are for students, tourists, people here on business, or those seeking to make America their permanent home. It is a daunting undertaking, given the volume of international travel to the United States. It also involves the coordination of multiple government entities, particularly the State Department and DHS, both of which are represented here today.

Since the 9/11 attacks against our country, there have been notable changes to strengthen our visa security, including recent adjustments made following the attacks in Paris and San Bernardino. For example, amid ISIS's growing online presence, the Department of Homeland Security is exploring ways to expand its use of social media to screen travelers seeking to enter the United States.

I look forward to hearing more about these efforts, and also about the contribution of ICE's visa security program that may help identify threats posed by potential travelers early on. We need to know if this program is adding real security and, if so, how to expand its reach.

As with all of our recent hearings, I expect that we will find elements of our visa security that we can improve upon – understanding that we can never eliminate all risk and should not turn our back on the many benefits of trade, travel and immigration. Yet as we continuously improve the security of our immigration system, we must also keep our eye on perhaps the even more pressing threat of homegrown terrorism.

For all that we do to strengthen our borders and our immigration security, groups like ISIS know all too well that they may bypass our multiple layers of homeland security by using online propaganda to recruit people already inside our borders to carry out attacks against the United States. In this respect, preventing ISIS's twisted propaganda from mobilizing our young people to carry out terrorist violence may help combat the long-term terrorist threats to the homeland in ways that aviation screening and watchlist checks can never do.

I look forward to our continued work on this committee on both combatting homegrown terrorism and strengthening the security of our immigration systems. And I hope we can use today's hearing to identify some common sense improvements to the security of visas. Thank you to the witnesses for your testimony and for your service to our country.

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.

U.S. Citizenship and Immigration Services

WRITTEN TESTIMONY

OF

LEON RODRIGUEZ
DIRECTOR
U.S. CITIZENSHIP AND IMMIGRATION SERVICES
DEPARTMENT OF HOMELAND SECURITY

FOR A HEARING ON

"The Security of U.S. Visa Programs"

BEFORE
THE U.S. SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

MARCH 15, 2016
10:00 A.M.
340 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC

Chairman Johnson, Ranking Member Carper, and distinguished members of the Committee, thank you for the opportunity to testify at today's hearing. While my colleagues from the Department of State (DOS) and the Department of Homeland Security's (DHS) Immigration and Customs Enforcement (ICE) will discuss security screening in the visa process, my testimony will focus specifically on U.S. Citizenship and Immigration Services' (USCIS) role in the security process for visa petitions and other USCIS adjudications. As the Director of USCIS, I work with the talented and dedicated professionals at my agency and throughout the federal government to secure America's promise as a nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, and ensuring the integrity of our immigration system. From the visa petition stage to post-entry applications for immigration benefits, USCIS works closely with DOS, the DHS partners represented on this panel, and others to ensure that those wishing to enter the United States are screened thoroughly and repeatedly in every instance and without exception. Security and integrity are central to USCIS's mission, and USCIS personnel work with steadfast resolve and vigilance to identify and deny benefits to immigration applicants who pose a threat to national security or public safety, or who attempt to gain benefits through fraud.

Visa Adjudication Overview

DHS and DOS both have roles to play in determining whether a foreign national will be issued a visa and admitted to the United States. Generally, a foreign national who seeks to enter the United States must first obtain a U.S. visa from DOS. In many instances these individuals must first have a petition filed and approved on their behalf with USCIS. However, certain international travelers may be eligible to travel to the United States without a visa if they meet the requirements for visa-free travel such as under the Visa Waiver Program (VWP). A foreign national who is issued a U.S. visa or is eligible for admission without a visa may travel to a U.S. air, sea, or land port of entry and apply for admission into the United States.

There are two broad classes of foreign nationals who are issued U.S. visas: nonimmigrants and immigrants. Nonimmigrant visas allow foreign nationals to travel to the United States on a temporary basis (for example, a vacation, temporary employment, or study and exchange). Immigrant visas allow foreign nationals, who have met the numerous eligibility requirements for lawful permanent residence, to travel to the United States for the purpose of residing in the country as lawful permanent residents (LPR). Individuals who have applied for humanitarian relief under the Immigration and Nationality Act (INA) are outside the scope of this testimony.

Most visits to the United States are made with a "B1/B2" nonimmigrant visa issued by DOS, or under the VWP or equivalent authority, for temporary stays for business or pleasure. The VWP is managed by U.S. Customs and Border Protection (CBP) and other DHS entities in consultation with DOS.

In those instances where USCIS is required under our law to adjudicate immigrant or nonimmigrant petitions, USCIS will carefully review the claimed basis for the petition (e.g., family or employment relationship). When USCIS approves such a petition for a beneficiary abroad, that information is communicated to DOS. The approval of such a petition does not give a foreign national any immigration status. It does not guarantee that DOS will issue a visa, and it is not a guarantee that CBP will admit the individual to the United States.

After USCIS has approved the petition under the appropriate visa classification, the beneficiary of the petition may then begin the visa application process with DOS. DOS is responsible for the adjudication of visa applications. As part of its adjudication process, DOS ensures that the applicant is eligible for a visa as an immigrant or nonimmigrant under the requested classification, and that the applicant is admissible to the United States. Once granted a visa, the foreign national may travel to the United States. On arrival at a U.S. port of entry, such as an airport, CBP inspects the individual and determines whether to admit the individual to the United States.

Visa Screening Responsibilities

DOS and DHS each have screening responsibilities as part of our respective roles in the visa process. USCIS screening during petition adjudication involves screening of both the petitioner and the foreign national beneficiary against law enforcement and national security lookouts and records. USCIS reviews each petition to determine if the petitioner and beneficiary meet the statutory requirements of the petition. Generally, this review is done to determine if the petitioner and beneficiary have the relationship claimed in the petition – either a family-based relationship, or employment-based. USCIS does not review petitions for admissibility to the United States. This is done initially by DOS prior to visa issuance and by CBP at time of entry. As such, any information uncovered is reviewed by USCIS and, if the petition is otherwise approvable, provided to our partners at DOS. Also, if there is an indication that a petitioner may have a conviction for a specified offense against a minor, as defined in the Adam Walsh Act, USCIS conducts a Federal Bureau of Investigation Fingerprint check of the petitioner.

My colleague from DOS will provide more detail on visa adjudication. However, DOS generally conducts an interview with the visa applicant and conducts additional biographic and biometric screening; including a battery of additional background security checks. If DOS issues the visa, the foreign national beneficiary must travel to the United States and apply for admission within the visa validity period, which varies depending upon the visa classification. At the port of entry, CBP conducts additional biographic and biometric screening and background security checks on these individuals, to determine their admissibility to the United States.

Applications for Immigration Benefits by Foreign Nationals Already in the United States

In some circumstances individuals admitted to the United States on nonimmigrant visas may be able to seek certain immigration benefits while in the United States. For example, a foreign national who was previously admitted to the United States as a nonimmigrant may seek to extend his or her stay or change his or her nonimmigrant status with USCIS if the individual meets the requirements for doing so. As a part of their request, these individuals are screened against law enforcement and national security lookouts and records. Any information uncovered is reviewed according to current agency policies. If the information uncovered indicates that the subject may have national security, criminal, or public safety concerns which make them removable from the United States, USCIS works closely with ICE and other law enforcement offices to ensure that appropriate actions are taken. Depending on the immigration classification sought, additional biographic checks may be conducted.

Moreover, certain foreign nationals in the United States, including some who were initially admitted on nonimmigrant visas, may be eligible under our immigration laws to adjust to lawful permanent resident status. Those eligible individuals must file a Form I-485 *Application to Register Permanent Residence or Adjust Status* with USCIS. The I-485 applicant must provide evidence of a USCIS-approved petition as the basis for immigration status, or concurrently file the immigrant petition with the I-485 application to establish the claimed family or employment relationship and/or classification specified under the INA, and meet all requirements for adjustment of status.

For each adjustment application, USCIS initiates a number of biographic and biometric security checks to establish eligibility for the benefit and admissibility to the United States. USCIS screens applicants against law enforcement and national security lookouts as well as FBI biographic and biometric holdings. Additionally, USCIS may interview the applicant to elicit information regarding identity, derogatory and conflicting information, involvement in terrorist or criminal activity, or other disqualifying factors.

Most individuals who become LPRs are allowed to apply for U.S. citizenship through the naturalization process after a given period of time. There is, however, a category of LPRs that must petition USCIS in order to retain their LPR status. Those who became LPRs on the basis of an Alien Entrepreneur Visa Petition and those who became LPRs on the basis of a marriage that occurred less than two years prior to the date they attained LPR status are considered conditional permanent residents. A conditional permanent resident must petition USCIS to remove the conditions on the residence within 90 days of the end of his or her second year as a conditional LPR. These individuals again undergo biographic and biometric security checks, and are screened against law enforcement and national security lookouts, records, and FBI biometric holdings. In addition, USCIS may also conduct interviews in the process of determining whether to lift conditions on permanent residence. Conditional permanent residence can be terminated due to information obtained during the interview and USCIS can share the information with ICE.

USCIS receives approximately 750,000 applications for naturalization each year. Many of these applicants were admitted into the United States as either immigrant or nonimmigrant visa holders. For each naturalization applicant, USCIS initiates a number of biographic and biometric security checks. USCIS screens applicants against law enforcement and national security lookouts and records as well as FBI biographic and biometric holdings. Additionally, all applicants for naturalization must be interviewed to establish their eligibility; this requirement may not be waived. During the interview, the officer confirms the basic biographic data and identity of the applicant, conducts an examination of the applicant's knowledge of the English language and of U.S. history and civics, with minor exceptions, and confirms that the applicant has no factors or activities that may make him or her ineligible for naturalization—such as certain types of criminal history, national security concerns, or prior false claims to U.S. citizenship. Information found in the interview can be used to deny the naturalization and can be shared with ICE for further investigation.

During the process of adjudicating any application, petition, or request filed with USCIS, if any national security concerns are raised, either based on security and background checks, personal interviews, testimony, or other sources, USCIS conducts an additional review through the internal Controlled Application Review and Resolution Program (CARRP). CARRP includes a

complete review of the case file and, in most cases, additional screening to ensure that eligibility is met. CARRP procedure includes regular supervisory review and headquarters coordination.

As part of the CARRP review process, USCIS also collaborates closely with its partners in the law enforcement and intelligence communities, including the Federal Bureau of Investigation, in order to review available information from these other U.S. Government entities and determine if it is relevant to eligibility and/or admissibility. This engagement is not one-sided, as USCIS also uses CARRP to alert relevant agencies that may wish to take action on the subject of the national security concern. It is USCIS policy to take any ongoing law enforcement activities into consideration prior to making a decision or taking action on any case with national security concerns.

Additional Coordination with Federal Partners

USCIS remains committed to ensuring that immigration benefits are not granted to individuals who pose a threat to national security or public safety, or who seek to defraud the U.S. immigration system. At its core, this system ensures that every application or petition for an immigration benefit is screened before it is adjudicated. As noted above, in support of these screening efforts, USCIS works closely with DOS, CBP, ICE, and other law enforcement partners. USCIS engages with law enforcement and Intelligence Community members for assistance with identity verification, acquisition of additional information, or deconfliction to ensure USCIS activities will not adversely affect an ongoing law enforcement investigation. USCIS also shares lead information, such as coordinating with ICE on potential human trafficking concerns associated with T and U nonimmigrant visas. USCIS continues to work with DHS's I&A, and other Intelligence Community elements, to enhance screening.

Conclusion

I appreciate the support and interest of this Committee in our efforts on these and other matters critical to the transparency, integrity, consistency, and efficiency of our immigration system and the work of USCIS.

I will be happy to answer your questions.

U.S. Immigration and Customs Enforcement

WRITTEN TESTIMONY

OF

SARAH R. SALDAÑA

DIRECTOR

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

"The Security of U.S Visa Programs"

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

Tuesday, March 15, 2016
342 Dirksen Senate Office Building

Introduction

Chairman Johnson, Ranking Member Carper, and distinguished members of the Committee:

Thank you for the opportunity to discuss the role of U.S. Immigration and Customs Enforcement (ICE) in the visa screening and vetting process. At ICE, we strive to uphold our homeland security mission by confronting dangerous challenges on a global stage, including threats emanating from beyond America's physical borders. I am proud and honored to serve alongside the dedicated men and women of ICE who work tirelessly to enforce our immigration and customs laws and keep this nation safe. Today, I welcome the opportunity to provide an overview of our international operations and highlight ICE's security programs that guard the nation against diverse and global threats.

One of ICE's three operational components – Homeland Security Investigations (HSI) – is responsible for the agency's work in vetting visa applications and working with our partners at the U.S. Department of State (DOS) and U.S. Citizenship and Immigration Services (USCIS). HSI's three operational priorities are border security, public safety, and counterterrorism/homeland security. HSI has extremely broad authorities and jurisdiction over the investigation of crimes with a nexus to U.S. borders and ports of entry. It investigates transnational crime by conducting a wide range of domestic and international criminal investigations, often in coordination with other local, state, federal, and international partners, targeting the illegal movement of people and merchandise into, within, and out of the United States. HSI investigates offenses that stem from our traditional customs and immigration authorities, including smuggling of illicit goods and people, and illicit finance associated with

global criminal organizations. These efforts provide a crucial layer of security vetting of individuals hoping to come to the United States.

The Visa Security Program and Pre-Adjudicated Threat Recognition Intelligence Operations Team

ICE strives to protect our nation's homeland security wherever threats confront us. One of our most important priorities is to detect and deter threats before they reach our nation's borders. To achieve this goal, ICE currently deploys approximately 250 Special Agents, 17 Deportation Officers, and 176 support staff to 62 offices in 46 countries. ICE's international staff works in conjunction with international law enforcement counterparts to detect, disrupt, and dismantle transnational criminal groups and individuals who seek to cause harm to the security of the United States.

The Homeland Security Act of 2002 authorizes the deployment of DHS officers to diplomatic posts to perform visa security activities and provide advice and training to DOS consular officers. This critical mission is accomplished by the Visa Security Program (VSP). VSP's primary purpose is to identify terrorists, criminals, and other individuals who are ineligible for visas prior to their travel or application for admission to the United States.

VSP is our first line of defense in the visa process against terrorists and criminal organizations by preventing foreign nationals who pose a threat to national security from entering the United States. The visa adjudication process is often the first opportunity to assess whether a potential visitor or immigrant poses a threat. Furthermore, the visa adjudication process is an ongoing and continuous vetting process that searches for derogatory information on applicants. No visa recipient is granted admittance based on a single review point.

Visa security is an important and collaborative function, shared by both DOS and DHS, including the component offices of ICE, U.S. Customs and Border Protection (CBP), and USCIS. Our components constantly seek to enhance our systems and processes to improve visa security efforts. Through the Pre-Adjudicated Threat Recognition Intelligence Operations Team (PATRIOT) initiative, we conduct automated screening of visa application information against DHS holdings, as well as holdings of other U.S. agencies, prior to the applicant's interview and visa adjudication. The process includes in-depth vetting of applicants identified as potentially having derogatory information who may be of investigative interest, or ineligible to receive U.S. visas. PATRIOT takes a risk-based approach and uses interagency resources from ICE, CBP, DOS, and the Intelligence Community to identify national security and public safety threats.

VSP differs from most other U.S. Government screening efforts in that it leverages its capabilities, such as in-person interviews, and works collaboratively with U.S. agencies at post to investigate suspect travelers, enhance existing information, and identify previously unknown threats instead of simply denying visas and any potential travel. In Fiscal Year (FY) 2015, VSP reviewed over two million visa applications, contributing input to approximately 8,600 cases in which visas were refused. Of these refusals, over 2,200 applicants had some known or suspected connection to terrorism or terrorist organizations.

In addition, VSP enhances visa vetting by increasing automated data exchange between DOS and the CBP National Targeting Center (NTC), which provides tactical targeting and analytical research to prevent terrorists from entering the United States. The flow of online visa information to DHS systems is now automated and information is sent back to DOS using an automated interface.

ICE also deploys personnel to the NTC to augment and expand current operations, and the co-location of personnel helps increase both communication and information sharing. The NTC conducts pre-departure vetting of all travelers on flights bound for the United States. This vetting identifies high-risk passengers who should be the subject of no-board recommendations to carriers, including those whose visas are later revoked.

Within VSP's international footprint, we deploy specially trained agents overseas to screen and vet visa applications at 26 high-risk locations in 20 countries, augmenting vetting mechanisms in place worldwide in order to enhance efforts at these critical posts to identify potential terrorist and criminal threats before they enter the United States. ICE accomplishes this crucial function by conducting targeted, in-depth reviews of individual visa applications and applicants prior to visa issuance, and making recommendations to consular officers to refuse or revoke visas when warranted. ICE actions complement the consular officers' screening, applicant interviews, and reviews of applications and supporting documentation. As a result of additional congressional funding in FY 2015, HSI expanded VSP operations to six new visa issuing posts.

Coordination with the U.S. Department of State

Effective border security requires broad information sharing and cooperation among U.S. government agencies. In October 2006, ICE entered into a memorandum of understanding (MOU) with the DOS Bureau of Consular Affairs in order to exchange visa and immigration data. The agreement allows ICE and DOS to exchange information contained in each agency's respective electronic databases pertaining to foreign persons seeking entry into the United States. This exchange of information allows DOS Consular Affairs personnel to query and access ICE

and CBP records. Consular Affairs personnel can then consider prior violations when adjudicating visa applications for persons who have applied to enter the United States.

Similarly, the exchange of information allows ICE personnel to query the DOS Consular Consolidated Database and to access passport and visa application information of persons under investigation by ICE. This information sharing also allows ICE to alert Consular Affairs personnel of ongoing criminal investigations for the purpose of visa adjudication.

In January 2011, ICE signed an MOU outlining roles, responsibilities, and collaboration between ICE, DOS Consular Affairs, and DOS's Diplomatic Security Service. To facilitate information sharing and reduce duplication of efforts, ICE and DOS conduct collaborative training and orientation prior to overseas deployments. At overseas posts, ICE and DOS personnel work closely together in working groups, meetings, trainings and briefings, and engage in regular and timely information sharing. Additionally, ICE and DOS personnel work side by side to identify embassies for potential future expansion of the VSP and routinely travel together and provide briefings to U.S. embassy personnel prior to commencement of operations.

Additional ICE Responsibilities in the Visa Process

ICE's role in the visa screening process does not end at the visa screening units. Rather, government screening efforts continue to examine visa holders before and during their authorized travel to the United States. For example, should a visa traveler match derogatory information within government holdings, DHS and DOS work collaboratively to determine if the information warrants DOS revocation of his/her visa regardless of whether the individual is outside or inside the United States, thereby, denying him/her any further travel access to our country. DHS also strives to ensure that only authorized visitors are entering the country, and

DHS components actively share with each other information gathered about admissibility indicators, intelligence records and additional information retrieved from travelers interviewed at secondary inspections stations at the ports of entry.

Overstay Enforcement in the United States

ICE actively identifies and initiates action against overstay violators who are enforcement priorities. ICE's primary objective is to vet system-generated leads in order to identify true overstay violators, match any criminal conviction history or other priority basis, and take appropriate enforcement actions. Within ICE, there are dedicated units, special agents, analysts, and systems in place to address nonimmigrant overstays. Through investigative efforts, ICE analyzes and determines which overstay leads may be suitable for further national security investigation.

From a DHS processing standpoint, ICE analyzes system-generated leads initially created by, or matched against, the data feed for biographical entry and exit records stored in CBP's Arrival and Departure Information System (ADIS). ADIS supports DHS's ability to identify nonimmigrants who have remained in the United States beyond their authorized periods of admission or have violated the terms and conditions of their visas. Once the leads are received, ICE conducts both batch and manual vetting against government databases, social media, and public indices. This vetting helps determine if an individual who overstayed has departed the United States, adjusted to a lawful status, or would be appropriate for an enforcement action.

As part of a tiered review, ICE prioritizes nonimmigrant overstay cases through risk-based analysis. HSI's Counterterrorism and Criminal Exploitation Unit (CTCEU) oversees the national program dedicated to the investigation of nonimmigrant visa violators who may pose a

national security risk and/or public safety concern. Each year, CTCEU analyzes records of hundreds of thousands of potential status violators after preliminary analysis of data from the various systems, including Student and Exchange Visitor Information System (SEVIS) and ADIS, along with other information. After this analysis, CTCEU establishes compliance or departure dates from the United States and/or determines potential violations that warrant field investigations.

CTCEU proactively develops cases for investigation in furtherance of the overstay mission, monitors the latest threat reports, and proactively addresses emergent issues. This practice, which is designed to detect and identify individuals exhibiting specific risk factors based on intelligence reporting, travel patterns, and in-depth criminal research and analysis, has contributed to DHS's counterterrorism mission by initiating and supporting high-priority national security initiatives based on specific intelligence.

In order to ensure that those who may pose the greatest threats to national security are given top priority, ICE uses intelligence-based criteria developed in close consultation with the intelligence and law enforcement communities. ICE chairs the Compliance Enforcement Advisory Panel (CEAP), which is comprised of subject matter experts from other law enforcement agencies and members of the Intelligence Community who assist the CTCEU in maintaining targeting methods in line with the most current threat information. The CEAP is convened on a quarterly basis to discuss recent intelligence developments and update the CTCEU's targeting framework in order to ensure that the nonimmigrant overstays and status violators who pose the greatest threats to national security are targeted.

Another source for overstay and status violation referrals is CTCEU's Visa Waiver Enforcement Program (VWEP). Visa-free travel to the United States builds upon our close

bilateral relationships and fosters commercial and individual ties among tourist and business travelers in the United States and abroad. The Visa Waiver Program (VWP) currently allows eligible nationals of 38 countries to travel to the United States without a visa and, if admitted, to remain in the country for a maximum of 90 days for tourism or business purposes. The VWEP, implemented in 2008, addresses overstays within the VWP population.

Today, CTCEU regularly scrutinizes a refined list of individuals who have been identified as potential overstays who entered the United States under the VWP. A primary goal of VWEP is to identify those subjects who attempt to circumvent the U.S. immigration system by seeking to exploit VWP travel.

Enforcement Priorities

Each year, the CTCEU receives approximately one million leads on nonimmigrants that have potentially violated the terms of their admission. Over half of these leads are closed due to the vetting conducted by analysts, which eliminates false matches and accounts for departures and pending immigration benefits. To better manage investigative resources, CTCEU relies on a prioritization framework established in consultation with interagency partners within the national intelligence and federal law enforcement communities through CEAP. On November 20, 2014, the Secretary of Homeland Security established priorities to focus enforcement and removal policies on individuals convicted of serious criminal offenses or who otherwise pose a threat to national security, border security, or public safety. To better manage its investigative resources, CTCEU has aligned its policy on sending leads to the field with the Secretary's priorities.

ICE's prioritization framework begins with a review and analysis to determine which immigration violators pose the greatest risks to our national security. CTCEU conducts an initial

review, dividing leads into 10 CTCEU priority levels. Priority Level 1, which focuses on the greatest risks, is based on special projects and initiatives to address national security concerns, public safety, and applying certain targeting rules. These projects and initiatives include: the Recurrent Student Vetting Program; DHS's Overstay Projects; Absent Without Leave (AWOL) Program; INTERPOL Leads; and individuals who have been watchlisted.

In FY 2015, CTCEU reviewed 971,305 leads regarding potential overstays. Numerous leads were able to be closed through an automated vetting process. The most common reasons for closure were subsequent departure from the United States or pending immigration benefits. A total of 9,968 leads were sent to HSI field offices for investigation – an average of 40 leads per working day. Of the 9,968 leads sent to the field, 3,083 are currently under investigation, 4,148 were closed as being in compliance (pending immigration benefit, granted asylum, approved adjustment of status application, or have departed the United States) and the remaining leads were returned to CTCEU for continuous monitoring and further investigation. In FY 2015 alone, HSI made 1,910 arrests, including 133 criminal arrests that resulted in 86 indictments and 80 convictions.

The remaining leads that cannot be closed by the automated vetting process and are not sent to HSI field offices for investigation are shared with one of ICE's other operational components – Enforcement and Removal Operations (ERO). When ERO receives this information, it forwards it to one of its three targeting centers, where the cases are once again vetted against criminal and national security databases, and additional leads may be generated. Those leads are then provided to ERO field offices for civil immigration enforcement action consistent with the priorities identified by the Secretary on November 20, 2014.

Conclusion

VSP is crucial to ICE's mission to protect the homeland. ICE is proud to work collaboratively with our DHS partners and our colleagues at DOS. Furthermore, ICE is committed to working with its U.S. Government and international partners and, especially, with the members of this Committee to forge a strong and productive relationship to help prevent and combat threats to our nation.

Finally, as ICE's operations continue to expand and evolve, we are constantly evaluating how best to accomplish our mission. Since ICE's establishment in 2003, ERO has experienced substantial growth and evolution in its mission. In addition, the ERO enforcement strategy has shifted heavily towards the investigation, identification, location, arrest, prosecution, and removal of individuals who present a danger to national security or threaten public safety, which may include some visa or Visa Waiver Program overstays.

Given these augmenting responsibilities, Secretary Johnson has directed ICE to work with the Department's Chief Human Capital Officer to review and determine whether changes need to be made to the agency's overtime compensation system for ICE officers. I am committed to working with the Department, the Office of Management and Budget, our employees, and Congress on any necessary next steps.

Thank you for the opportunity to testify about these important issues. I would be pleased to answer any questions you may have.

OFFICE OF INSPECTOR GENERAL

Testimony of Inspector General John Roth

Before the Committee on Homeland Security and Governmental Affairs

United States Senate

"The Security of U.S. Visa Programs"

Homeland Security

March 15, 2016
10:00 AM

DHS OIG HIGHLIGHTS

The Security of U.S. Visa Programs

March 15, 2016

Why We Did This

The audits and inspections discussed in this testimony are part of our ongoing efforts to ensure the efficiency and integrity of DHS' immigration programs and operations. Our criminal investigators also regularly investigate fraud within the benefits approval process, often involving a corrupt USCIS employee.

What We Recommend

We made numerous recommendations to DHS and its components—primarily USCIS and ICE—in these reports. Our recommendations were aimed at improving the effectiveness and implementation of visa programs.

For Further Information:
Contact our Office of Legislative Affairs at (202) 254-4100, or email us at DHS-OIG.OfficeLegislativeAffairs@oig.dhs.gov

What We Found

This testimony highlights a number of our recent reviews related to U.S. visa programs. Our findings include:

- After 11 years, USCIS has made little progress in transforming its paper-based processes into an automated immigration benefits processing environment. USCIS now estimates that it will take three more years and an additional $1 billion to automate benefit processing. This delay will prevent USCIS from achieving its workload processing, national security, and customer service goals.

- Known human traffickers used work and fiancé visas to bring victims to the U.S. using legal means. USCIS and ICE can improve data sharing and coordination regarding suspected human traffickers to better identify potential trafficking cases.

- ICE did not have sufficient data to determine the effectiveness of its Visa Security Program, which requires the screening and vetting of overseas visa applicants.

- The laws and regulations governing the EB-5 immigrant investor program do not give USCIS the authority to deny or terminate a regional center's participation in the program due to fraud or national security concerns.

DHS Response

With few exceptions, DHS and its components concurred with recommendations in these reports.

Chairman Johnson, Ranking Member Carper, and Members of the Committee, thank you for inviting me to discuss my office's oversight of the Department of Homeland Security's visa programs and components responsible for administering and enforcing visas. Our recent work has involved a number of audits and investigations. I will discuss each of the audits, as well as a representative sample of some of our investigations.

Information Technology Transformation

This week, we published our sixth report since 2005 on U.S. Citizenship and Immigration Services' (USCIS) efforts to transform its paper-based processes into an integrated and automated immigration benefits processing environment.[1] This program is a massive undertaking to modernize processing of approximately 90 immigration benefits types. The main component of the Transformation Program is the USCIS Electronic Immigration System (ELIS), intended to provide integrated online case management to support end-to-end automated adjudication of immigration benefits. Once implemented, individuals seeking an immigration benefit should be able to establish online ELIS accounts to file and track their applications, petitions, or requests as they move through the immigration process.

We undertook this audit to answer a relatively simple question: after 11 years and considerable expense, what has been the outcome of USCIS' efforts to automate benefits processing? We focused on benefits processing automation progress and performance outcomes. We interviewed dozens of individuals, including over 60 end-users in the field who are using ELIS, and reviewed voluminous source documents.

The answer, unfortunately, is that at the time of our field work, which ended in July 2015, little progress had been made. Specifically, we found that:

- Although USCIS deployed ELIS in May 2012, to date only two of approximately 90 types of immigration benefits are available for online customer filing, accounting for less than 10 percent of the agency's total workload. These are the USCIS Immigrant Fee, which allows customers to submit electronic payment of the $165 processing fee for an immigrant visa packet, and the Application to Replace Permanent Resident Card (Form I-90).

[1] *USCIS Automation of Immigration Benefits Processing Remains Ineffective*, (OIG 16-48, March 2016).

- Among the limited number of USCIS employees using ELIS, personnel reported that the system was not user friendly, was missing critical functionality, and had significant performance problems processing benefits cases. Some of those issues are set forth in this chart:[2]

USCIS ELIS User Feedback on I-90 Processing	
• Need to manually refresh website often to see the most recent information. • Difficulty navigating among multiple screens and web browsers. • Inability to move browser windows to view case data. • Cases getting stuck throughout the process and inability to move to the next step without intervention. • Inability to undo a function or correct a data entry error. • Inability to enter comments on actions taken after a case has been adjudicated.	• Card errors received when "NMN" is entered for applicants with no middle name.* • Failure to produce cards for approved cases. • Inability to process benefits for military or homebound applicants. • Errors in displaying customer date of birth.* • Scheduling applicants to submit biometrics (photo, signature, prints) that are not needed.* • Inability to create a case referral electronically once adjudication is complete.

- The limited ELIS deployment and current system performance problems may be attributed to some of the same deficiencies we reported regarding previous USCIS IT transformation attempts. To date, the USCIS has not ensured sufficient stakeholder involvement in ELIS implementation activities and decisions for meeting field operational needs. Testing has not been conducted adequately to ensure end-to-end functionality prior to each ELIS release. Further, USCIS still has not provided adequate post-implementation technical support for end-users, an issue that has been ongoing since the first ELIS release in 2012.

- As it struggles to address these system issues, USCIS now estimates that it will take three more years—over four years longer than estimated—and an additional $1 billion to automate all benefit types as expected. Until USCIS fully implements ELIS with all the needed improvements, the agency will remain unable to achieve its workload processing, customer service, and national security goals. Specifically, in 2011, USCIS

[2] USCIS has indicated that the issues marked with an asterisk were addressed during the time of our audit. Because of the nature of the audit process, we are unable to validate that this has occurred.

established a plan to implement ELIS agency-wide by 2014. However, USCIS was not able to carry out this plan and the schedule was delayed by four years, causing a program breach. An updated baseline schedule for the Transformation Program was approved in April 2015; however, USCIS also shifted and delayed these release dates.

- Certain program goals have also not been met. According to agency-wide performance metrics, benefits processing in ELIS was to take less than 65 days. However, we found that as of May 2015, processing was taking an average of 112 days, almost twice that amount of time. Previous results reported for this metric also were high: 104 days in November 2014, 95 days in February 2015, and 112 days in May 2015. By slowing down the work of adjudicators, ELIS was resulting in less efficiency and productivity in processing benefits.

Similarly, in 2014, we reported that although ELIS capabilities had been implemented, the anticipated efficiencies still had not been achieved. In fact, we reported in 2014 that adjudicating benefits on paper was faster than adjudicating them in ELIS. This remains unchanged to date. Ensuring progress in operational efficiency was hampered by the fact that USCIS lacked an adequate methodology for assessing ELIS' impact on time and accuracy in benefits processing. Beyond obtaining feedback from personnel and customers using the system, the Transformation Program Office could not effectively gauge whether cases were being adjudicated more efficiently or accurately in ELIS.

We acknowledge that DHS has taken significant steps to improve the process by which it introduces new information technology, including moving from a traditional waterfall methodology to a new, incremental methodology, called Agile. We also acknowledge that implementation of automation is very much a moving target, and that USCIS may have since made progress on the problem in the time since the fieldwork of our audit ended in July 2015.

Human Trafficking and the Visa Process

In January of this year, we issued a report on human trafficking and the visa process.[3] Our audit objectives were to determine how individuals charged or convicted of human trafficking used legal means to bring victims to the United States, and to identify data quality and exchange issues that may hinder efforts to combat human trafficking. We conducted this audit as part of our "Big Data"

[3] *ICE and USCIS Could Improve Data Quality and Exchange to Help Identify Potential Human Trafficking Cases*, (OIG 16-17, January 2016).

initiative, in which we compare datasets from different DHS components (or other government databases outside of DHS) to attempt to gain insights into potential issues in DHS programs and operations.

In this audit, we compared databases from two components—Immigration and Customs Enforcement (ICE) and USCIS. ICE's Case Management System, which is housed in the larger Customs and Border Protection TECS system, contains information on human trafficking investigations conducted by Homeland Security Investigations. USCIS uses two databases: (1) the Humanitarian Adjudication for Victims Enterprise Nationwide (HAVEN) system to maintain information on visas granted to victims of human trafficking (U visas and T visas), and (2) the Computer Linked Application Information Management System (CLAIMS3) to process immigrant and nonimmigrant applications and petitions—such as work and family reunification visa requests.

As a result of comparing the data in these databases, our auditors came to the following conclusions:

- Work and fiancé visas were the predominant means that human traffickers used to bring victims into the United States legally. We made this determination based on matching ICE's human trafficking data against USCIS' data on visa petitions. Specifically, 17 of 32 known human trafficking cases we identified involved the use of nonimmigrant work visas and fiancé visas; the remaining 15 victims entered the United States illegally or overstayed their visitor visas. In one example, fiancé visas were used to lure human trafficking victims to the United States as part of marriage fraud schemes. The traffickers confiscated the victims' passports and subjected them to involuntary servitude, forced labor, and/or forced sex.

- Family reunification visas also were possibly used to bring victims into the country. From 2005 through 2014, 274 of over 10,500 (3 percent) of the subjects of ICE human trafficking investigations successfully petitioned USCIS to bring family members and fiancés to the United States. Because ICE data included investigations that were still ongoing and did not reflect whether the final conviction resulted in a human trafficking or lesser charge, ICE could not tell us exactly how many of the 274 individual visa petitioners were human traffickers. However, ICE data showed that 18 of the 274 had been arrested for human trafficking-related crimes.

- ICE and USCIS could improve data quality to facilitate data matching and identification of possible instances of human trafficking. For example, ICE had to extensively manipulate its system to provide us with reasonably reliable data for our data matching and analysis. USCIS did not always collect names and other identifiers of human traffickers that victims had provided in their T visa applications. Due to incomplete data, we were limited in our ability to match, analyze, and draw conclusions from the components' databases.

- We found that ICE and USCIS cooperated on a limited basis to exchange human trafficking data, but concluded that opportunities existed for improved data exchange between ICE and USCIS.

We made three recommendations to improve the effectiveness of the programs to identify human traffickers and their victims. ICE and USCIS have concurred with the recommendations. The three recommendations are still open, and both ICE and USCIS are taking actions to resolve them. We are satisfied with the progress thus far.

DHS Visa Security Program

In September of 2014, we published a report about the DHS Visa Security Program.[4] The program, which was established by Congress, requires DHS personnel stationed overseas, specifically ICE Special Agents, to perform visa security activities in order to prevent terrorists, criminals, and other ineligible applicants from receiving U.S. visas. Specifically, they are required to screen and vet visa applicants to determine their eligibility for U.S. visas. This is largely done through a screening process which compares visa application data held by the Department of State with a DHS law enforcement database – TECS – to determine whether there are any matches. In Fiscal Year (FY) 2012, ICE agents screened over 1.3 million visa applicants. Those applicants with a match are then vetted, which involves researching and investigating the visa applicant, examining documents submitted with the visa application, interviewing the applicant, and consulting with consular, law enforcement, or other officials. ICE special agents vetted more than 171,000 visa applicants in FY 2012.

Additionally, ICE agents are required to provide advice and training to consular officers about security threats relating to adjudicating visa applications.

As a result of our inspection, we found:

[4] *The DHS Visa Security Program*, (OIG-14-137, September 2014).

- The effectiveness of the Visa Security Program cannot be determined. Notwithstanding that ICE was required to develop measures to assess performance, it has not taken appropriate actions to ensure that (1) data needed to assess program performance is collected and reported, (2) appropriate advice and training is provided to consular officers, and (3) the amount of time needed for visa security related activities at each post is tracked and used in determining staffing and funding needs. As a result, ICE is unable to ensure that the Visa Security Program is operating as intended.

  At the time of our inspection, ICE senior management officials expressed a lack of confidence in the value of the current performance measures. As a result, these performance measures were not included in the DHS and ICE annual reporting of performance.

- ICE has not consistently or effectively provided training or expert advice to consular officers as required. In interviewing consular officers we learned that much of the training provided did not cover critical subjects needed to enhance their skills. Additionally, during our site visits we found a number of embassies where the consular officers have not been provided with any training, or training on a sporadic basis.

- It is unknown how much time ICE agents assigned to the program actually spend on visa security issues. Agents do not record the amount of time they spend on this activity, notwithstanding that ICE had received special funding to institute the program. Anecdotally, we found some agents spent very little time on visa security activities, while agents in other posts spent a high percentage of their time on it.

- The Visa Security Program expansion has been slow. At the time of our report, only 20 of the 225 visa-issuing posts had visa security units. According to program officials, Visa Security Program expansion has been constrained by budget limitations, difficulties obtaining visas for certain countries, State's mandate to reduce personnel overseas, and objections from State Department officials at some posts due to security concerns or space limitations.

We made 10 recommendations to improve the effectiveness of the program. ICE concurred with each of them. Currently, ICE has accomplished five of those recommendations, and is working to accomplish the remaining five. While

progress has been slow, we are currently satisfied with ICE's activities in this regard.

Investor Visa Program

In December of 2013, we published an audit report on challenges facing the EB-5 program, which administers visas for immigrant investors.[5] Through the EB-5 Program, foreign investors have the opportunity to obtain lawful, permanent residency in the U.S. for themselves, their spouses, and their minor unmarried children by making a certain level of capital investment and associated job creation or preservation. The EB-5 program requires that the foreign investor make a capital investment of either $500,000 or $1 million, depending on whether or not the investment is in a high unemployment area. The foreign investors must invest the proper amount of capital in a business, called a new commercial enterprise, which will create or preserve at least 10 full-time jobs, for qualifying U.S. workers, within 2 years of receiving conditional permanent residency.

The purpose of our audit was to determine whether USCIS administered and managed the EB-5 Regional Center Program (regional center program) effectively. We found:

- The laws and regulations governing the program do not give USCIS the authority to deny or terminate a regional center's participation in the EB-5 program based on fraud or national security concerns. At the time of the audit, USCIS had not developed regulations that apply to the regional centers in respect to denying participation in the program when regional center principals are connected with questionable activities that may harm national security.

- Additionally, USCIS has difficulty ensuring the integrity of the EB-5 regional center program. Specifically, USCIS does not always ensure that regional centers meet all program eligibility requirements, and USCIS officials interpret and apply the Code of Federal Regulations (CFR) and policies differently. USCIS did not always document decisions and responses to external parties who inquired about program activities causing the EB-5 regional center program to appear vulnerable to perceptions of internal and external influences.

[5] *United States Citizenship and Immigration Services' Employment-Based Fifth Preference (EB-5) Regional Center Program*, (OIG-14-19, December 2013).

- USCIS is unable to demonstrate the benefits of foreign investment into the U.S. economy. Although USCIS requires documentation that the foreign funds were invested in the investment pool by the foreign investor, the implementing regulation does not provide USCIS the authority to verify that the foreign funds were invested in companies creating U.S. jobs. Additionally, the regulation allows foreign investors to take credit for jobs created by U.S. investors.

As a result, USCIS has limited oversight of regional centers' business structures and financial activities. For example, we identified 12 of 15 regional center files in which USCIS allowed the creation of new commercial enterprises that collected EB-5 capital to make loans to other job-creating entities. USCIS adjudicators confirmed that because the CFR does not give them the authority to oversee these additional job creating entities, they are unable to inquire or obtain detail that would verify foreign funds are invested in the U.S. economy via a job-creating entity.

Additionally, one regulation allows foreign investors to take credit for jobs created with U.S. funds, making it impossible for USCIS to determine whether the foreign funds actually created U.S. jobs. Consequently, the foreign investors are able to gain eligibility for permanent resident status without proof of U.S. job creation. In one case we reviewed, an EB-5 project received 82 percent of its funding from U.S. investors through a regional center. The regional center was able to claim 100 percent of the projected job growth from the project to apply toward its foreign investors even though the foreign investment was limited to 18 percent of the total investment in the project.

We made four recommendations to improve the effectiveness of the program. Two of those recommendations have been closed. The other two are pending: one is for a study to be done to assess the effectiveness of the EB-5 program, which is being completed by the Department of the Commerce and is scheduled to be completed shortly; the second is update regulations to provide greater clarity regarding USCIS' authority to deny or terminate EB-5 regional center participants at any phase of the process because of national security and/or fraud risks. They would also make it explicit that fraud and national security concerns can constitute cause for revocation of regional center status; give USCIS authority to verify that foreign funds were invested in companies creating U.S. jobs; and ensure requirements for the EB-5 regional center program are applied consistently to all participants. This recommendation is overdue, and we are in discussions with USCIS as to when this action will be completed.

Our 2013 findings were reinforced and confirmed by an audit released by the Government Accountability Office (GAO) in August of last year.[6] In that audit, GAO found that the EB-5 program has both fraud and national security risks that USCIS needs to correct. For example, GAO found:

- Limitations in electronic data USCIS collects on regional centers and immigrant investors limits their usefulness in conducting fraud-mitigating activities. Certain basic information, such as name, date of birth and address are either not entered into electronic databases or are not standardized, so basic fraud-related searches cannot be conducted.

- USCIS anti-fraud personnel conduct only limited site visits, and GAO recommends increasing the number of site visits to regional centers and program sites to look for indicia of fraud.

- USCIS does not conduct interviews of immigrant investors to who they award permanent residency, which the GAO believes would assist in establishing whether the investor is a victim of or complicit in fraud.

- USCIS has significant limitations on being able to verify the source of the money invested and, other than by self-certification, does not have a reliable basis to determine whether the money is from an improper source.

The GAO also found (as had the previous OIG audit) that USCIS' practice of allowing immigrant investors to claim jobs generated by investments from other sources overstates the economic benefit of the EB-5 program. The GAO found that, in the one project they looked at, many immigrant investors would not have qualified for lawful permanent residency without the practice of allowing them to claim jobs created by all investments in the commercial enterprise, regardless if they were EB-5 investors.

Other Audits Involving the Visa Process

We have published a number of different audits. Some of those audits may be less relevant either because of the passage of time or a change in circumstances. However, we will briefly describe them here.

[6] *Immigrant Investor Program: Additional Actions Needed to Better Assess Fraud Risks and Report Economic Benefits,* (GAO-15-696, August 2015).

In August of 2013, we published an audit report regarding USCIS' handling of the L-1 visa program.[7] The L-1 visa program facilitates the temporary transfer of foreign nationals with management, professional, and specialist skills to the United States. We found that USCIS adjudicators were inconsistently deciding L-1 petitions because of inadequate guidance from USCIS headquarters, particularly as it relates to the requirement that the petitioner have "specialized knowledge." Additionally, we found one regulation, which permits a foreign company to receive an L-1 visa for an employee to start a "new office" in the United States. We found that this provision is "inherently susceptible to abuse."

In June of 2013, we published an audit report regarding USCIS' tracking of potentially fraudulent applications for family-based immigration benefits.[8] U.S. immigration law grants permanent resident status to aliens who legally marry a U.S. citizen or lawful permanent resident and to certain aliens who are family members of U.S. citizens or lawful permanent residents. We performed an audit to determine whether USCIS recorded information about adjudicated family-based petitions and applications suspected of being fraudulent according to agency policy requirements and in a manner that deterred immigration fraud.

We found that USCIS has procedures to track and monitor documentation related to petitions and applications for family-based immigration benefits suspected of being fraudulent. However, once family-based immigration petitions and applications were investigated and adjudicated, fraud-related data were not always recorded and updated in appropriate electronic databases to ensure their accuracy, completeness, and reliability. Specifically, USCIS personnel did not record in appropriate electronic databases all petitions and applications denied, revoked, or rescinded because of fraud. Supervisors also did not review the data entered into the databases to monitor case resolution. Without accurate data and adequate supervisory review, USCIS may have limited its ability to track, monitor, and identify inadmissible aliens, and to detect and deter immigration benefit fraud.

Finally, in November 2012, we published a report about the visa waiver program, which allows nationals from designated countries to enter the United States and stay for up to 90 days without obtaining a visa from a U.S. embassy or consulate.[9] The purpose of our review was to determine the adequacy of processes used to determine (1) a country's initial designation as a Visa Waiver

[7] *Implementation of L-1 Visa Regulations*, (OIG 13-107, August 2013).
[8] *U.S. Citizenship and Immigration Services' Tracking and Monitoring of Potentially Fraudulent Petitions and Applications for Family-Based Immigration Benefits*, (OIG-13-97, June 2013).
[9] *The Visa Waiver Program*, (OIG-13-07, November 2012).

Program participant, and the continuing designation of current Visa Waiver Program countries; and (2) how effectively the Visa Waiver Program Office collaborates with key stakeholders. We determined that the Visa Waiver Program Office had established standard operating procedures and review criteria that satisfy the goals for conducting country reviews. Although Visa Waiver Program officials maintained effective collaboration with stakeholders during the review process, additional efforts are needed to communicate with appropriate officials the standards needed to achieve compliance with Visa Waiver Program requirements and the criteria used to assess compliance. In addition, challenges that may reduce the effectiveness of the Visa Waiver review process include untimely reporting of results, current staffing levels within the Visa Waiver Program Office, and its location in the DHS organizational structure.

Criminal Investigations

Our criminal investigators regularly investigate fraud within the benefits approval process, often involving a corrupt USCIS employee. We investigate a fairly steady stream of such conduct. The following are recent examples of the results of our investigations:

- Martin Trejo, a DHS contractor, was convicted for theft of government property, among other crimes, after a DHS OIG investigation determined that he stole approximately 1,000 blank, genuine USCIS I-797 Notice of Action forms over a five-year period for which he was paid approximately $5,000. Trejo delivered the forms to a civilian who then provided them to a fraudulent document broker.

- Efron DeLeon, a USCIS Immigration Services Assistant in Orlando, Florida, was convicted of obstruction of justice and false statements after a DHS OIG investigation found he illegally assisted immigration petitioners and beneficiaries at the Orlando USCIS Field Office. DeLeon destroyed records in alien files and provided information on how to circumvent questions in a USCIS marriage fraud interview. He also improperly accessed and viewed records in the Central Index System, a DHS database, and made false statements to DHS OIG investigators.

- Cassandra Gonzalez, non-DHS employee, was sentenced for her role in an immigration fraud scheme. Gonzalez and her conspirators, one of which was a former USCIS employee, facilitated false marriages, complete with fake documentation, to illegally obtain immigration benefits.

- Fernando Jacobs, a Supervisory Immigration Services Officer, and his co-conspirator, an Immigration Services Officer, were convicted of conspiracy, bribery, and other related crimes after a DHS OIG investigation revealed he accepted bribes to issue Lawful Permanent Resident cards to illegal aliens and accessed government databases to obtain information regarding USCIS applicant status.

- Richard Quidilla, a USCIS contractor, was convicted of unlawful procurement of citizenship and other related crimes after an OIG investigation determined that he unlawfully accessed USCIS databases in excess of authority and deleted names and biographical information of 28 bona fide naturalized US citizens, and inserted names and biographical information of individuals who either violated terms of their visas (over-stays) and/or were undocumented aliens. Once altered, the USCIS database falsely depicted the identities of the individuals inserted by the contractor as actual United States citizens.

Other matters

Additionally, as we have in the past, we receive information from DHS employees, which may uncover deficiencies in programs and operations in the visa program, or constitute a violation of law, regulation, and policy. The specifics of some of those complaints are protected from disclosure by the *Inspector General Act* and the *Whistleblower Protection Act*, particularly during the pendency of our investigation of those claims. However, I want the Committee to know that we take each of these claims seriously and will investigate them to the fullest extent possible. We will also take steps to protect whistleblowers from retaliation wherever we find it.

Conclusion

Deciding and administering immigration benefits, including visas, is a massive enterprise. USCIS alone uses about 19,000 people to process millions of applications for immigration benefits. They are required to enforce what are sometimes highly complex laws, regulations, and internal policies. They are rightly expected to process decisions within a reasonable time frame. USCIS and the rest of DHS accomplish their mission while working with an antiquated system of paper-based files more suited to an office environment from 1950 rather than 2016. This system creates inefficiencies and risks to the program. To give you an idea of the scope of the problem, USCIS spends more

that $300 million per year shipping, storing, and handling over 20 million immigrant files.

The size and complexity of the mission, coupled with an archaic method of processing applications, brings with it significant risk. There is risk to operations – in that it makes it more difficult for USCIS accomplish their mission. We found, for example, that the time to process immigration benefits was twice that of the metrics that USCIS established. Our earlier report on USCIS IT systems, published in July of 2014, reported that using the electronic files in use at the time took twice as long as using paper files.

Additionally, the present system presents risks to our national security – in that we may be admitting individuals who wish to do us harm, or who do not meet the requirements for a visa. Basic information on visa applicants was not captured in electronic format and thus cannot be used to perform basic investigative steps. Also, because of the poor quality of the electronic data kept by both USCIS and ICE, it was difficult to engage in data matching, which we believe is an effective tool in rooting out fraud and national security risks.

Mr. Chairman, this concludes my prepared statement. I am happy to answer any questions you or other Members of the Committee may have.