OFFICE OF INSPECTOR GENERAL

DHS Tracking of Visa Overstays is Hindered by Insufficient Technology

Homeland Security

May 1, 2017

OIG-17-56

DHS OIG HIGHLIGHTS

DHS Tracking of Visa Overstays Is Hindered by Insufficient Technology

May 1, 2017

Why We Did This Audit

DHS has primary responsibility for identifying visa overstays and taking enforcement action to address security risks. We conducted this audit to determine the effectiveness of Immigration and Custom Enforcement's (ICE) information technology (IT) systems to review, track, and share information associated with visas.

What We Recommend

We made three recommendations to the DHS CIO and two to the ICE CIO to improve information sharing, provide training and guidance, evaluate data reliability, and implement a biometric exit solution.

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

What We Found

Department of Homeland Security IT systems did not effectively support ICE visa tracking operations. ICE personnel responsible for investigating in-country visa overstays pieced together information from dozens of systems and databases, some of which were not integrated and did not electronically share information. Despite previous efforts to improve information sharing, the DHS Chief Information Officer (CIO) did not provide the oversight and centralized management needed to address these issues. Additionally, ICE did not ensure that its field personnel received the training and guidance needed to properly use the systems currently available to conduct visa overstay tracking.

Further, the Department lacked a comprehensive biometric exit system at U.S. ports of departure to capture information on nonimmigrant visitors who exit the United States. Without a complete exit system, DHS relied on third-party departure data, such as commercial carrier passenger manifests, to confirm a visitor's departure from the country. However, these commercial sources occasionally provided false departure or arrival status on visitors.

Because of these systems and management limitations, DHS could not account for all visa overstays in data it annually reported to Congress. Manual checking across multiple systems used for visa tracking contributed to backlogs in casework and delays in investigating suspects who potentially posed public safety or homeland security risks.

Management Response

The DHS CIO and ICE CIO concurred with our recommendations.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

May 1, 2017

MEMORANDUM FOR: The Honorable Richard Staropoli
Chief Information Officer
Department of Homeland Security

Michael C. Brown
Chief Information Officer
Office of the Chief Information Officer
U.S. Immigration and Customs Enforcement

Shonnie Lyon
Director
Office of Biometric Identity Management
National Protection & Programs Directorate

Donald W. Neufeld
Associate Director
Service Center Operations
U.S. Citizenship and Immigration Services

Phillip A. Landfried
Assistant Commissioner
Office of Information and Technology
U.S. Customs and Border Protection

FROM: Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *DHS Tracking of Visa Overstays is Hindered by Insufficient Technology*

Attached for your action is our final report, *DHS Tracking of Visa Overstays is Hindered by Insufficient Technology*. We incorporated the formal comments from the Department in the final report.

The report contains five recommendations aimed at improving the tracking of visa overstays by DHS. The Department concurred with all of our recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Once your office has fully implemented the recommendations, please submit a formal closeout request to us within 30 days so that we may close the recommendations. The request should be accompanied by evidence of completion of agreed-upon corrective actions.

Please email a signed PDF copy of all responses and closeout requests OIGITAuditsFollowup@oig.dhs.gov. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Kristen Bernard, Director, Information Technology Management, at (202) 254-0962.

Attachment

Table of Contents

Background 1
Results of Audit 7
Fragmented IT Systems Hindered Efficient and Effective Overstay Tracking..... 7
Recommendations 17
Lack of an Exit System Hampered DHS' Ability to Capture Accurate Departure Data 17
Recommendations 21
Unintegrated Systems and the Lack of an Exit System Resulted in Poor Overstay Reporting and Inefficient Tracking..... 21

Appendixes

Appendix A: Objective, Scope, and Methodology..... 29
Appendix B: Management Comments to the Draft Report..... 31
Appendix C: IT Systems Used for Visa Tracking by ICE Headquarters and Field Personnel.....35
Appendix D: Office of IT Audits Major Contributors to This Report..... 38
Appendix E: Report Distribution..... 39

Abbreviations

ADIS	Arrival and Departure Information System
APIS	Advance Passenger Information System
ATS-P	Automated Targeting System-Passenger
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
CLAIMS	Computer Linked Application Information Management System
CTCEU	Counterterrorism and Criminal Exploitation Unit
ERO	Enforcement and Removal Operations
GAO	Government Accountability Office
HSI	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
IT	information technology
OBIM	Office of Biometric Identity Management
OMB	Office of Management and Budget
OIG	Office of Inspector General
RAPS	Refugees, Asylum and Parole System
SEVIS	Student and Exchange Visitor Information System
UPAX	Unified Passenger
USCIS	U.S. Citizenship and Immigration Services

Background

Each year, millions of foreign nationals come to the United States legally on a temporary basis with a nonimmigrant visa. According to the Department of State, more than10.8 million nonimmigrant visas were issued in fiscal year 2015. The Department of State issues a visa as an endorsement on a passport, indicating that the holder is allowed to enter the country and remain for a specified period of time.

Visa holders are required to depart from the United States on or before the designated admit until date, which ranges in time depending on the specific visa classification. U.S. Customs and Border Protection (CBP) designates the admit until date at the port of entry. If a foreign national wishes to remain in the country legally beyond an admission period, he or she must file a petition for extension or a change in status with U.S. Citizenship and Immigration Services (USCIS) before the admission period expires. Certain groups cannot apply for extensions, such as participants in the Visa Waiver Program and those who have violated their terms of admission.[1]

When a nonimmigrant visitor is admitted to the country under a specific nonimmigrant category but exceeds the authorized period of admission, the visitor becomes an "overstay." The visitor may be categorized as an in-country overstay (a foreign national whose admit until date had passed and who is suspected of still being physically present in the United States) or an out-of-country overstay (a foreign national who departed the United States after the admit until date had passed). Federal law establishes consequences for visitors who overstay their authorized periods of admission.[2] According to Department of Homeland Security reports, only a small percentage of visa holders overstayed their admission periods in 2015; however, their impact on national security can be great. For example, two of the 19 hijackers on September 11, 2001, were visa overstays. This prompted the 9/11 Commission to call for the government to ensure that all visitors to the United States are tracked on entry and exit.

DHS has primary responsibility for identifying visa overstays and taking enforcement action to address security risks. ICE is the lead component in DHS responsible for immigration enforcement within the United States and holds primary responsibility for in-country nonimmigrant visa overstay tracking and enforcement. However, multiple components also play a role in

[1] Violations and prohibitions include the following: visa has expired at the time of petition for extension, petitioner committed a crime while on a visa, petitioner did not enter the United States legally, or petitioner's passport will not be valid throughout the course of his or her stay in the United States.
[2] 8 United States Code 1182(a)(9)(B); 1227(a)(1)(C)(i); 1202(g).

tracking, investigating, apprehending, and deporting removable aliens, including visa overstays, as depicted in table 1.

Table 1: Roles and Responsibilities for Managing Overstays

Agency	Responsibility
U.S. Customs and Border Protection (CBP)	Collects biographic and biometric information to document arrival and departure information on individuals arriving in the United States at U.S. ports of entry. CBP officers also determine nonimmigrant admissibility into the United States and provide an "admit until date," by which time the individual must leave the country to avoid overstaying. CBP publicly reports the number of visitors who overstayed their visa in a given year.
U.S. Citizenship and Immigration Services (USCIS)	Receives, processes, and maintains documentation pertaining to a visa holder's immigration status, including the extension or change of status, and works with U.S. Immigration and Customs Enforcement (ICE) to ensure proper adherence to U.S. immigration laws.
National Protection and Programs Directorate's Office of Biometric Identity Management (OBIM)	Stores biometrics, such as fingerprints, in order to confirm an individual's identity and determine whether the individual is on a watch list for terrorists, criminals, or immigration violators. OBIM is the lead entity within the Department for biometric identity services.
U.S. Immigration and Customs Enforcement (ICE)	Responsible for overstay enforcement operations.[3] • The **Homeland Security Investigations (HSI)** office investigates domestic and international activities arising from the illegal movement of people and goods into and out of the United States. Within HSI, the **Counterterrorism and Criminal Exploitation Unit (CTCEU)** is responsible for investigating nonimmigrant overstays, including potential national security risks and violators of nonimmigrant visas. CTCEU assigns leads that warrant further investigation to agents located in one of the HSI domestic field offices. • The **Enforcement and Removal Operations (ERO)** office apprehends confirmed overstay aliens who are subject to removal from the United States, detains these individuals when necessary, and removes them from the country. ERO officers performed a total of 235,413 removals in FY 2015.
Department of State	Responsible for receiving, vetting, and processing applications for immigration and temporary admission to the United States from abroad. Overseas consular offices obtain documentation, conduct interviews with applicants, and issue immigrant and nonimmigrant visas to approved applicants. The Department of State collaborates with ICE HSI as part of the Visa Security Program to screen and vet visa applicants.

Source: Office of the Inspector General (OIG)-generated based on DHS and Department of State data

[3] DHS Delegation Number 7030.2, *Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement* (November 13, 2004).

DHS Automated Process for Identifying Nonimmigrant Visa Holders

The Department of State issues visas to immigrant and nonimmigrant applicants prior to their arrival to the United States. Once visa holders arrive to the United States and are admitted by CBP, they must depart within their lawful period of admission if they have not been granted an extension or change of status by USCIS.

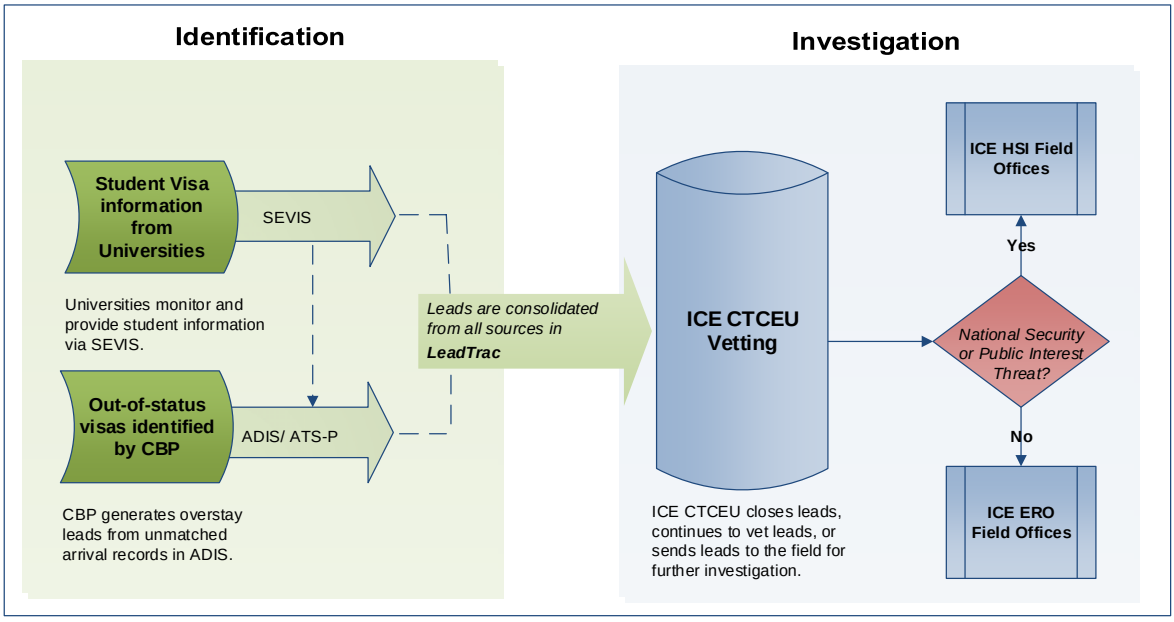
The Department has an electronic process for identifying nonimmigrant visa holders who may have remained in the country beyond the period of their admission. A suspected overstay is automatically flagged in DHS' systems when there is no record of nonimmigrant departure and subsequent vetting shows no change in visitor status prior to the end of the authorized admission period. There are three primary DHS systems that support this automated overstay identification process.

- DHS identifies individuals as overstays primarily by electronically matching records of visitor entry to and exit from the United States in the Arrival and Departure Information System (ADIS).
- DHS identifies student visa violators and exchange violators through data that universities input directly to ICE's Student and Exchange Visitor Information System (SEVIS), which transmits data to ADIS.
- Leads identified in ADIS and SEVIS are vetted against national security vetting data in the Automated Targeting System-Passenger (ATS-P) as well as the National Counterterrorism Center. These leads are fed into CTCEU's case management system, LeadTrac.[4]

The overstay identification process is pictured in figure 1.

[4] LeadTrac is not an abbreviation.

Figure 1: High Level Process to Identify and Investigate Overstay Leads



Source: OIG-generated based on DHS data

ICE's Manual Process for Investigating Overstays

Following this automated overstay identification process, CTCEU analysts conduct additional investigations as needed to determine whether an individual has actually overstayed his or her authorized admission period. Specifically, analysts conduct extensive research to gather foreign national biographic data — such as name, date of birth, and country of citizenship — as well as analyze any additional records relevant to each case. For example, CTCEU analysts may search for travel records on a suspected overstay, compare biometrics obtained before or during entry to the country against DHS' biometric storage system, and search for applications in USCIS' immigration processing systems. This type of cross-functional tracking and investigation helps ICE personnel to compile a complete picture, with evidence, to confirm whether a subject is a visa overstay. Conversely, this data may provide evidence that a subject departed the country on time or received an immigration benefit to extend a visa, and thus is no longer an overstay.

This manual vetting process helps CTCEU analysts confirm the priority of each case already assigned by the automated lead generation process. In each case, CTCEU may close the lead, continue to monitor the lead, or determine where the lead should be sent for further investigation. Leads that are determined not to be national security or public safety threats are sent to ERO for additional review. Leads that cannot be resolved or closed by CTCEU, and that pose a

threat to national security or public safety, are sent to HSI agents located in field offices for review, investigation, and potential apprehension and arrest of subjects.

In FY 2015, CTCEU received more than 970,000 leads on possible overstays. The continuous automated vetting process, pictured previously in figure 1, enabled ICE to remove more than 825,000 leads from priority lists. The 145,001 remaining leads were considered valid national security leads and were processed by CTCEU in FY 2015, as pictured in table 2.

Table 2: Nonimmigrant Visa Leads Processed by Automated Vetting in FY 2015

Total leads that were sent to CTCEU in FY 2015	**971,305**
Total leads that were removed by automated vetting (Individuals who had departed the U.S. or complied with immigration law)	[141,344]
Total leads that were sent to ERO	[684,960]
Total leads remaining that were processed by CTCEU in FY15	**145,001**

Source: OIG-generated based on DHS data

Prior Audit Reports on Visa Overstays

The Government Accountability Office (GAO) has conducted three audits on DHS visa tracking operations since 2011.

- In 2011, GAO reported on DHS' tracking and processing of visa overstays and concluded there was a backlog of 1.6 million un-reviewed, unmatched arrival records.[5] Additionally, GAO found that DHS was unable to publish a report on annual overstay rates due to data integrity issues. Specifically, they found that a lack of a biometric exit system inhibited the reliability of departure information. GAO recommended that DHS create a timeline for improving overstay enforcement procedures and metrics, examine the feasibility of improving collection of departure forms, and broaden automated alerts for visa overstays. GAO closed these recommendations.

- In 2013, GAO reported on DHS' efforts to resolve these issues and found continued problems hampering DHS' attempts to reduce the unmatched

[5] *Additional Mechanisms for Collecting, Assessing and Sharing Data Could Strengthen DHS's Efforts but Would Have Costs,* GAO-11-411, April 2011.

arrival records backlog and efforts to shore up data reliability.[6] At the time of the audit, the backlog totaled more than one million records. Chief among the problems was the continued lack of a biometric exit system at U.S. ports of entry and departure. Additionally, GAO found that DHS still did not have accurate reporting on departures at land border crossings. DHS stated that a report on annual overstay figures would be released in December 2013.[7] GAO recommended that DHS review and resolve ongoing data integrity issues and establish milestones for implementing a biometric exit capability. GAO closed these recommendations.

- In 2017, GAO reported on DHS' efforts to develop a biometric exit solution to collect biometric data and report on potential overstays.[8] Since 2013, CBP has conducted four pilot programs to further the development and implementation of a biometric exit system. The GAO found that CBP had made progress in testing biometric exit capabilities, but faced longstanding planning, infrastructure, and staffing challenges to develop and implement a biometric exit system. Additionally, GAO found that DHS had improved overstay reporting by, among other actions, enhancing the systems it used to process entry and exit biographic data for potential overstays. GAO did not issue recommendations with this report.

In 2014, OIG reported on the effectiveness of DHS' visa security program in preventing ineligible applicants from receiving visas.[9] However, we determined that the issues disclosed did not specifically relate to the information systems DHS uses for visa tracking.

---

[6] *Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Air Exit Program*, GAO-13-683, July 2013.
[7] DHS did not meet the 2013 target for releasing the overstay report. The first overstay report was published in January 2016.
[8] *DHS Has Made Progress in Planning for a Biometric Exit System and Reporting Overstays, but Challenges Remain*, GAO-17-170, February, 2017.
[9] *The DHS Visa Security Program*, DHS OIG-14-137, September 10, 2014.

Results of Audit

DHS' IT systems did not effectively support ICE visa tracking operations. ICE personnel responsible for investigating in-country visa overstays pieced together information from dozens of systems and databases, some of which were not integrated and did not electronically share information. Despite previous efforts to improve information sharing, the DHS Chief Information Officer (CIO) did not provide the oversight and centralized management needed to address these issues. Additionally, ICE did not ensure that its field personnel received the training and guidance needed to properly use the systems currently available to conduct visa overstay tracking.

Further, the Department lacked a comprehensive biometric exit system at U.S. ports of departure to capture information on nonimmigrant visitors who exit the United States. Without a complete exit system, DHS relied on third-party departure data, such as commercial carrier passenger manifests, to confirm a visitor's departure from the country. However, these commercial sources occasionally provided false departure or arrival status on visitors.

Because of these systems and management limitations, DHS could not account for all visa overstays in data it annually reported to Congress. Manual checking across multiple systems used for visa tracking contributed to backlogs in casework and delays in investigating suspects who potentially posed public safety or homeland security risks.

Fragmented IT Systems Hindered Efficient and Effective Overstay Tracking

The myriad of information systems and databases used in DHS for visa tracking were not effective in identifying nonimmigrant overstays. Some of these systems and databases were "stove-piped" and did not electronically share information, resulting in numerous inefficiencies. Despite some recent system integration efforts, ICE personnel conducted cumbersome and manual searches across multiple systems for information on in-country overstays. ICE personnel periodically were unsure of which system to use and were hampered by multiple passwords required to maintain system access. Obtaining visa and immigration status on suspected overstays also was difficult due to the unstructured manner in which data were stored.

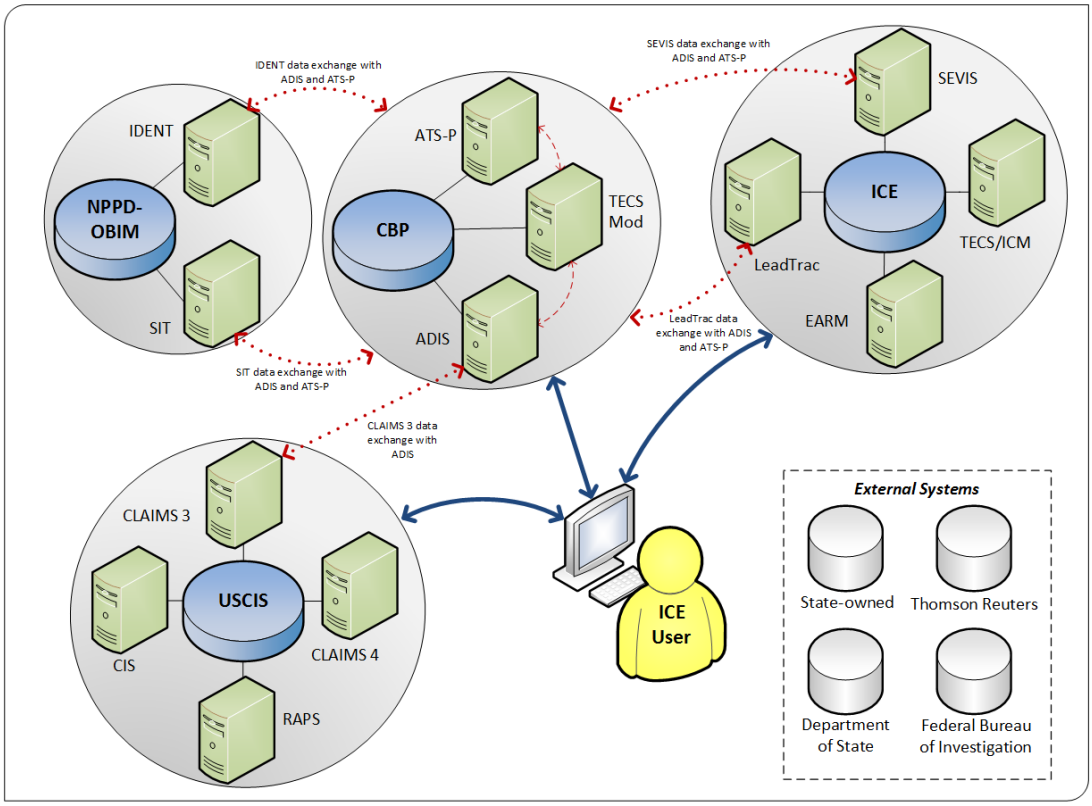
Numerous Unintegrated IT Systems Used for Visa Tracking

Multiple legacy information systems and databases used in DHS for visa tracking did not fully support ICE's efforts to identify nonimmigrant visitor overstays. Federal law requires the CIO of each department or agency to develop and maintain a sound IT environment to ensure integration across IT capabilities used for mission operations.[10] However, DHS has not fully established a shared and integrated IT environment to promote collaboration across components, which hinders effective and efficient visa mission operations.

Up to 27 distinct DHS information systems and databases were used to support the Department's visa-related programs and operations, depending on location. The Department has worked to integrate some IT systems used for tracking arrivals and departures and for capturing derogatory information. However, ICE personnel still need to check multiple individual systems to accurately determine an individual's overstay status. For example, CTCEU analysts at ICE headquarters relied on approximately 17 systems, including 13 DHS and 4 external systems and databases, as depicted in figure 2. ICE personnel in the field used as many as 18 distinct DHS systems and databases, as well as approximately 5 external systems, to conduct their investigations.

[10] *National Defense Authorization Act for Fiscal Year 1996*, Pub. L. No. 104–106 (1996). OMB Memorandum 15-14, *Management and Oversight of Federal Information Technology*, June 10, 2015.

Figure 2: DHS Visa IT Systems Used by CTCEU Analysts [11]



Source: OIG-generated based on DHS data

The external systems depicted are owned by other Federal agencies such as the Department of State and the Federal Bureau of Investigation, individual state agencies, and a private research entity (i.e., Thomson Reuters). In addition to ADIS and ATS-P, CBP manages TECS (not an acronym) for border screening. Apart from SEVIS, ICE has three case management systems: LeadTrac, TECS Investigative Case Management, and ENFORCE Alien Removal Module. USCIS' immigrant benefits processing systems include the Computer-Linked Application Information Management System (versions 3 and 4), the Central Index System, and the Refugees, Asylum and Parole System (RAPS). National Protection and Programs Directorate's Office of Biometric Identity Management manages the Automated Biometric Identification System (IDENT) used to store

[11] DHS systems used by CTCEU analysts include the Automated Biometric Identification System (IDENT); ADIS; Modernized TECS (not an acronym); Secondary Inspection Tool (SIT); ATS-P; ENFORCE Alien Removal Module; Investigative Case Management System/TECS; LeadTrac; SEVIS; Computer Linked Application Information Management System 3.0 and 4.0 (CLAIMS 3 and 4); Refugees, Asylum and Parole System (RAPS); and the Central Index System.

all of the Department's biometric data such as fingerprints and the Secondary Inspection Tool for entry/exit screening.

Some of these systems and databases are "stove-piped," meaning they are maintained by separate components within the Department and typically were not designed or retrofitted to ensure integration or interoperability. DHS components have taken steps to integrate systems used for visa tracking. However, ICE personnel remain encumbered by having to search multiple systems to obtain information directly from each source. Having to access and search among numerous systems to carry out their overstay tracking responsibilities can be daunting for the individual systems' users. For example, ICE agents at one field location reportedly relied on as many as 16 distinct systems and databases to investigate, classify, and locate visa overstays. A listing of IT systems used for visa tracking can be found in appendix C.

The lack of complete integration and information sharing has produced numerous inefficiencies. Many systems were designed and built for a distinct purpose, these systems contain only the fields of information relevant for performing the functions necessary to support that purpose. In some cases, this information is not shared among the various systems, meaning that ICE agents and analysts pull information together from multiple IT systems to "connect the dots" when conducting investigation queries. For example, CTCEU analysts reported having to sometimes check data in up to17 different systems to conduct an initial investigation for each lead before making a determination on an overstay status. This includes searching across multiple DHS systems (CBP, USCIS, and ICE) and external systems to gather key data elements for each individual, such as country of origin, immigration status, and criminal history. In each case, CTCEU personnel must gather information to compile a case file before a lead can be confirmed and passed along to HSI agents in the field for investigation.

Also, because each system has a different or unique purpose, HSI and ERO personnel in the field were not always sure which systems to use to perform their specific job functions. For example, an ICE agent with more than 20 years of experience that we interviewed was not aware of a system commonly used by other ICE personnel to search data on national security vetting results. Further, ICE personnel also were not always aware of the various USCIS systems that could be used for visa tracking. Personnel we met at multiple locations expressed concerns that they were unaware of all systems available to them across DHS components and agencies, potentially limiting their effectiveness in carrying out their visa tracking responsibilities.

The lack of integration also posed problems for users needing to access the various systems. For example, ICE personnel had to retain and use anywhere from 10 to 40 passwords, which was cumbersome as users may log into dozens of systems each week, all with separate passwords. Users at every location we visited stated that the repeated log-ins from system to system took time and was often frustrating. Also, passwords expire on different dates, requiring that users take time to manage them. The sheer number of passwords using different protocols (i.e., mix of numbers, symbols, and upper and lower case letters) made it difficult to remember the passwords. As a result, users write the passwords down for easy reference, which poses a security risk.

Maintaining multiple passwords also increased the potential for denial of access and system lock-outs due to password expiration. In some cases, system lock-outs could be resolved with a 5-minute call to the system-specific helpdesk. Other circumstances required ICE agents and officers to wait hours before they were able to regain access, further slowing their searches. In one case, an ICE agent was locked out of a system for an entire day for his password to be reset; another agent estimated it could take 2 days to regain access to a system. In worst case scenarios, ICE agents stated that they had to avoid using systems they were locked out of and instead relied on coworkers to access these systems for them.

Immigration Status Data Were Not Well-Structured or Easily Accessible

ICE agents and officers faced challenges obtaining real-time access to information about the immigration status of potential overstays, which is critical to properly validate whether or not a subject is in the United States legally at the time of investigation. For instance, ICE needs to know when a foreign national under investigation files a petition or application to change his or her nonimmigrant status (extend the time allowed in the country). Foreign nationals may also be in the process of filing asylum applications, or obtain permission to remain in the country through permanent resident status, citizenship, or employment authorization. Having access to immigration status data for each individual under investigation is important for ICE to make the correct determination of overstay status. Timely and accurate data is especially critical given the high volume of immigration applications received each year. In FY 2015, USCIS received almost 84,000 asylum applications from more than 117,000 foreign nationals seeking permission to remain in the United States.

However, obtaining timely immigration status information has proven difficult due to the unstructured manner in which data are stored. Specifically, USCIS employs nearly a dozen unintegrated systems to manage its immigration benefits processing. Because USCIS systems are “forms-driven” rather than

"person-centric," each system is designed to process a particular application rather than to support all transactions associated with a single applicant. Consequently, ICE personnel had to conduct searches in multiple USCIS systems to compile the complete history of an individual and determine his or her current immigration status. These inefficiencies were further magnified by the lack of notifications built into USCIS systems, meaning that ICE did not receive an automated alert when a subject under investigation filed an application or received a benefit. This lengthened the amount of time required to search each system — multiple times in some cases — to determine a potential overstay's immigration status. Field personnel told us that searching across multiple USCIS systems was a long, cumbersome process that could take several hours, or several days, depending on the case.

Obtaining immigration status was even more problematic when ICE personnel could not gain access to some USCIS systems. For example, several agents and officers we interviewed were unable to access the RAPS system or CLAIMS 4. USCIS management representatives stated that access to this system was provided on a need-to-know basis. When an ICE user could not access this system, or in the event that immigration files had not been scanned or digitized, the user had to request the required information from USCIS personnel via hard copy. ICE agents and officers complained that the wait time could sometimes stretch to weeks or more, which delayed each case from moving forward and potentially resulted in investigations of overstay subjects that USCIS has already approved for changes of status. Conversely, USCIS personnel stated that the time to deliver a hard copy immigration file typically ranged from 2 to 8 work days, depending on the priority of the requested file. Nonetheless, such manual data exchanges caused delays in closing cases and moving on to new investigations.

Lastly, USCIS' CLAIMS 3, used to store immigration benefit application data, was not updated in a timely manner. For example, USCIS did not typically update CLAIMS 3 data as paper applications were received. Instead, according to USCIS' Office of Information Technology personnel, immigration benefit applications were sent to a vendor's facility where contractors open, scan, and enter application data for processing. This process could take up to 3 days, followed by another 1- or 2-day lag before ICE had access to view this data. This resulted in ICE personnel having to check the system multiple times to obtain updated application status and thereby make a visa overstay determination.

In 2006, USCIS created a consolidated search capability, the Person Centric Query Service, to provide a single search capability for immigration and naturalization applications and transactions. Although several ICE agents and

officers found the service beneficial and comprehensive, personnel at four field locations were unaware of it or lacked access to the system. Other ICE users questioned the reliability or completeness of the data returned when using this query service. Others said that it did not include all the details they needed for visa overstay tracking purposes. Therefore, ICE users felt compelled to double check the same data in legacy systems, such as CLAIMS 3 or the Central Index System, to confirm or look for more in-depth information.

Unintegrated Systems Used for Visa Overstay Tracking Persist in the Decentralized IT Environment

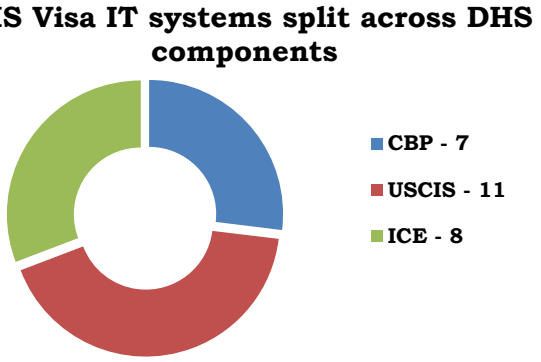
The stove-piped systems used for visa tracking were inherited from the former Immigration and Naturalization Service, which was abolished with the creation of DHS in 2003. Despite efforts to improve visa system integration and information sharing, the CIO has not provided the necessary oversight and the centralized management needed to overcome the fragmentation of its assets, as we have repeatedly reported.[12] Additionally, the ICE CIO has not provided adequate training or guidance to personnel in the field on how to properly use these IT systems to carry out visa overstay tracking.

DHS Legacy Systems Were Not Effectively Consolidated

In general, DHS inherited its fragmented IT systems environment from the former Immigration and Naturalization Service. With the creation of DHS in 2003, the Immigration and Naturalization Service was abolished and subsequently split into three separate components: CBP, ICE, and USCIS — each with distinct immigration and visa-related missions. Each component carried forward the legacy Immigration and Naturalization Service systems it needed to accomplish its respective mission responsibilities and support specific logistical and security requirements. One exception was TECS, which came from the Department of Treasury, but this system also was tailored within CBP and ICE to meet the components' specialized needs. Over time, distinct IT infrastructures evolved within each of the components, resulting in dozens of parallel and highly specialized visa-related IT systems. Figure 3 depicts the number of systems used by each component for visa-related operations.[13]

[12] *Improvements Needed to DHS' Information Technology Management Structure,* DHS OIG-04-30, July 2004*; Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain,* DHS OIG-08-91, September 4, 2008*; DHS Information Technology Management Has Improved, But Challenges Remain,* DHS OIG-12-82, May 4, 2012.
[13] This does not include IDENT, which is owned by the National Protection and Program Directorate.

Figure 3: Visa Tracking Systems Owned By The Former Immigration and Naturalization Service



Source: OIG-generated based on DHS data

Although DHS applications and networks resided on a common platform and in shared data centers, component IT systems lacked integration and were still maintained independently by each component CIO. Each component also independently managed its corresponding IT maintenance schedules, IT support services, contractors and vendors, software licenses, and user access policies.

Over time, a number of these systems have been updated or modernized 'in-house' within each component. In some cases, such as USCIS' Person Centric Query Service, entirely new systems were designed, developed, and implemented. Coordination across DHS stakeholders to gather requirements or obtain input was not always done to ensure individual component systems could support external user needs. We asked multiple ICE field office representatives whether requirements input had been requested during system upgrade or system development efforts and found that only two of nearly a dozen locations had been offered this opportunity. As an exception, CBP had a visa overstay working group in place at the time of our audit. Established in 2011, this working group was focused on enhancing the visa overstay vetting process and biographic exit capabilities. It also worked with ICE to reduce the time needed to identify and vet potential overstays by implementing upgrades to systems such as LeadTrac, SEVIS, and ADIS.

In 2012, CBP began an effort to consolidate 34 disparate data sources into a single system, Unified Passenger (UPAX). This effort was meant to upgrade a CBP system currently used by ICE for overstay vetting, and further integrate the numerous systems owned by CBP, USCIS, ICE, and the Department of State and thereby reduce the time required to review data on visa applicants planning to travel to the United States. Many of the systems that shared information with UPAX were the same systems ICE personnel used for visa

tracking. However, at the time of our audit, CBP had not identified all potential users DHS-wide based on mission need. Consequently, the system was not accessible to ICE field users to support their overstay investigations. None of the HSI agents or ERO field officers we interviewed had access to UPAX; some were unaware of its existence.

Centralized Oversight Was Lacking

Greater oversight and centralized management were needed to address the fragmented and unstructured visa IT environment. DHS policy states that the DHS CIO will oversee, manage, and consolidate all Department IT systems.[14] The Office of Management and Budget (OMB) also instructs CIOs to focus on eliminating duplication and to rationalize their agency IT investments, including mission and business IT systems.[15] Based on these guidelines, each agency CIO holds a key position in overseeing and directing how IT can best support mission operations, and ensuring collaboration and information sharing across component organizations.

The DHS CIO had several methods for ensuring consolidation of agency IT investments, but these had not yet been fully executed for visa IT systems. One such method is the Department's enterprise architecture approach, which includes broad, department-wide reviews of all IT systems used in a specific mission area, known as a "segment architecture."[16] The reviews are meant to establish a baseline architecture, or a blueprint and inventory of all systems used to perform common functions or capabilities across all components. Although the DHS CIO had established nearly 21 segment architectures since 2011, no segment architecture for visa IT capabilities had been created.

The DHS CIO has worked in coordination with the Department's components to improve information sharing among the various systems, such as SEVIS and ADIS, used for visa tracking. For example, in 2013, the DHS CIO was part of a department-wide task force that examined how the vetting and sharing of information associated with visa overstays could be improved. The task force focused on enhancing communication between components to reduce data redundancy and the need to conduct manual checks. The CIO reported that the work done on this task force increased information sharing between at least two systems that are used to identify overstays.

---

[14] DHS Management Directive 142-02-001, *Information Technology Integration and Management,* February 6, 2014.
[15] OMB Memorandum 11-29, *Chief Information Officer Authorities,* August 8, 2011.
[16] Segment architecture is a standard term for a particular set of IT functions that are used for one purpose.

Guidance for Field Personnel Was Inadequate

Because ICE personnel often use over a dozen systems, additional guidance was needed to support visa tracking in the field. ICE personnel we spoke with did not know how to use the tools and technology available for overstay tracking despite OMB direction that users of Federal IT resources have the skills, knowledge, and training needed to be effective.[17] For example, ICE officials were not familiar with the distinct functions and capabilities offered within each system used for overstay tracking. Some ERO officers were unclear on how to use ATS-P, CBP's automated passenger tracking system, to search for potential overstays or determine whether individuals had boarded flights to leave the country. ERO officers at a separate location did not know how to add information on an overstay case to the TECS law enforcement database, commonly used across CBP and ICE. As a result, DHS personnel did not have access to all the information available to make informed decisions. ICE personnel could not conduct efficient or effective visa tracking to the extent that they did not know how to fully utilize system functionality and capabilities as intended.

Further, ICE personnel lacked policies or guidance on appropriate system use. All but one of the ICE personnel we interviewed in the field were unable to locate any agency-wide, official guidance or checklists on systems used for visa tracking. Additionally, ICE management had not provided field users with documented procedures on which systems should be used to perform various steps of the investigative process. A reference list of 76 systems was available on the internal ICE intranet and included systems used for day-to-day administrative operations and training, as well as visa tracking systems. However, this did not include instructions on the potential uses of each system to accomplish the various visa overstay tracking responsibilities.

Lastly, additional training was needed for ICE field personnel to learn how to use systems for overstay tracking, as well as become familiar with the distinct search functions associated with each system. For example, field staff at one location explained that systems like TECS and CLAIMS contain specific functions or data fields that may provide additional information on an overstay lead. These were commonly known and understood by primary users within the component that owned the system, but were unfamiliar to external users. ICE field personnel expressed concerns that they might miss information due to a lack of training on system functionality and features.

[17] OMB Circular A-130, *Managing Information as a Strategic Resource*, Section 5(c)(3) (July 28, 2016).

We determined that ICE offered training for new hires through the Federal Law Enforcement Training Center; however, this training covered only a few IT systems owned or used by ICE for visa tracking. ICE field personnel also had access to training online or through informal coaching methods. Nevertheless, ICE personnel in the field did not consider this training sufficient because of the online "click through" format and the lack of hands-on learning opportunities.

Recommendations

Recommendation 1: We recommend the DHS CIO continue to work with components to further eliminate duplication, improve information sharing, and properly align system access, especially for system modernization efforts, across DHS according to visa tracking mission requirements.

Recommendation 2: We recommend that the ICE CIO assess and address the visa IT training needs of ICE users, including coordinating with system owners in other components to ensure that ICE users have the opportunity to receive official, hands-on training on these components' visa IT systems as well.

Recommendation 3: We recommend that the ICE CIO compile an up-to-date inventory of all IT systems across the Department that ICE agents and officers can use for visa tracking and provide documented guidance on potential uses of each system to accomplish the various visa overstay tracking responsibilities.

Lack of an Exit System Hampered DHS' Ability to Capture Accurate Departure Data

DHS lacked a completed exit system to capture biometric data on nonimmigrant visitor air and land departures from the country. DHS was required to implement a biometric air entry-exit system for tracking foreign nationals by 2009.[18] However, to date, DHS has not completed this effort due to funding and infrastructure challenges. Without a complete exit system, including the ability to obtain biometrics from visitors departing the country, DHS relied on third-party biographic data, such as commercial carrier passenger manifests, to confirm an individual's exit from the country. However, the effectiveness of this process depended on the accuracy of the third-party commercial carriers' records, which sometimes provided false departure status on individuals.

[18] 8 United States Code 1187 (8)(A)(i)

Exit System Not Completed as Required

The Department lacked a system at U.S. ports of departure to capture needed data on exiting foreigners. ICE field personnel we interviewed commonly cited this as the most significant gap in the Department's ability to conduct visa overstay tracking. As CBP officials repeatedly testified before Congress, the component lacked the personnel, facilities, and technology needed to account for travelers leaving the country. For example, airports in the United States had no designated areas or checkpoints to collect biometric data for travelers departing the country. Likewise, biometric land departure information was not captured, as most travelers crossed the borders to Mexico on foot or using their own vehicles and typically were not stopped for inspection.[19] Additionally, biographic information is not regularly captured on the southern border. By agreement, the Canadian Government captured biographic data on individuals crossing the northern border into Canada and shared this information with CBP Border Patrol; however, it excluded data on Canadian citizens traveling from the United States.[20]

DHS was required to implement a biometric entry-exit system for tracking foreign nationals by 2009, but has not completed this effort.[21] Specifically, Congressional mandates required the design and implementation of an integrated system that would provide foreign national arrival and departure biometrics for immigration control, enforcement, and reporting. To illustrate, such data were needed by entities such as CBP to determine visitor admissibility and departure, by Department of State consular offices responsible for visa processing, and by ICE for visa enforcement. DHS began a program to develop this entry and exit system in 2003.[22] Despite multiple pilots, such as the US-VISIT pilot program for exit systems at airports in 2009, virtually no progress was made prior to 2013. Moreover, GAO reported that DHS struggled to implement the exit system due to ineffective technology program management, design, and implementation practices.[23]

---

[19] CBP is able to reconcile a portion of travelers who arrive through the borders with Canada and Mexico, because many of those are frequent travelers whose reentrance to the United States confirms their previous departure.
[20] *United States-Canada Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness*, Action Plan, December 2011.
[21] 8 United States Code 1187 (8)(A)(i).
[22] The U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program was established in 2003 to develop a means for collecting biographic and biometric data on foreign nationals passing through U.S. ports of entry and departure.
[23] *Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Air Exit Program,* GAO-13-683, July 2013; *Key US-VISIT Components at Varying Stages of Completion, but Integrated and Reliable Schedule Needed,* GAO-10-13, November 2009; *Visa Waiver Program: Actions Are Needed to Improve Management of the Expansion Process, and to Assess and Mitigate Program Risks,* GAO-08-967, September 2008; *Homeland Security: Planned Expenditures for U.S. Visitor and Immigrant Status Program Need to Be Adequately Defined and Justified,* GAO-07-278, February 2007.

In 2013, because of the lack of progress, Congress transferred responsibility for research and development of the biometric exit system to CBP.[24] Since that time, CBP has initiated several pilots to test different technologies and capabilities, such as facial recognition, iris scans, and mobile fingerprint collection devices.

At the time of our audit, a biometric exit system pilot was underway at Atlanta's Hartsfield-Jackson International Airport. For this pilot effort, CBP combined traveler and airline data with real time images of travelers departing the country to confirm departure. CBP reported that the confirmation rate was approximately 98 percent for travelers who had their picture taken at their departure date. CBP plans to begin implementing the biometric exit system in 2018 at a number of airports with the highest volume of travelers. CBP officials anticipate that this system will provide more reliable data on departing travelers and a mechanism for complete and accurate matching of entry/exit records.

Recent legislation increased oversight requirements for Department CIOs across the Federal Government.[25] As a result, the DHS CIO is currently implementing additional oversight plans to monitor and provide feedback on major IT programs, such as the biometric exit system, before acquisition decisions are made.

Reliance on Third-Party Data on Departing Visitors

In the absence of a comprehensive biometric exit system at all U.S. ports of departure, DHS relied on third-party departure data, such as commercial carrier passenger manifests, to confirm an individual's exit from the country.[26] Identifying overstays involved matching this third party exit data against biographic and biometric data collected at land, air, and sea ports of entry.

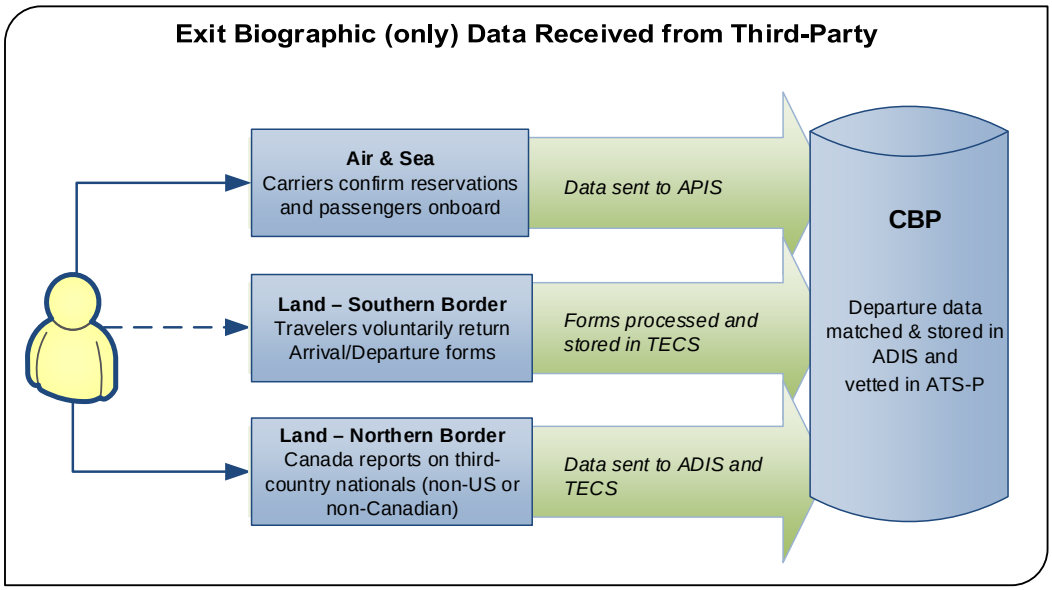
Specifically, CBP collected biographic and biometric data such as fingerprints from travelers entering the United States, and recorded it in DHS systems, including ADIS, TECS, and/or IDENT.[27] CBP receives commercial passenger and crew biographical data directly from air and sea carriers through the Advance Passenger Information System (APIS) prior to the passenger and crew's arrival in or departure from the United States. APIS then shares the data

---

[24] *Consolidated and Further Continuing Appropriations Act, 2013*, Pub. L. No. 113-6 (2013).
[25] Public Law 113-291.
[26] Commercial carriers are required by law to submit passenger manifests to CBP, which are then recorded as arrivals or departures from the United States.
[27] Biographic data is stored in ADIS or TECS, and biometric data is stored in IDENT.

with ADIS, which works as a central repository and automatically matches arrival and departure records for the purpose of identifying potential overstays. Both ADIS and APIS share information with ATS-P. ATS-P vets arrival and departure information and is used by ICE personnel to confirm a passenger's onboard status. DHS' process for capturing and checking exit data is depicted in figure 4.

Figure 4: DHS Process to Compile Exit Data[28]



Source: OIG-generated based on DHS data

The effectiveness of this process depended on the accuracy of records that DHS obtained from third-party commercial carriers, which occasionally provided incorrect departure or arrival status on individuals. Although CBP reported that ADIS had over a 90 percent match rate for individuals who entered the country by any given means and then departed by air, officials acknowledged data quality issues with specific commercial airline carriers. HSI agents and ERO officers also complained of multiple instances of false ADIS reporting on departures. For example, ADIS sometimes falsely reported (1) that individuals were still in the country after they had already departed, or (2) that individuals had left the country when they were still physically present in the United States. The latter occurred when airlines or other commercial carriers

[28] CBP uses other data collection and data sources to track departures from the United States. This includes CBP scanning documents of visitors departing the United States on the Northern and Southern borders during periodic "Pulse and Surge" operations which is tracked in TECS and shared with ADIS. Additionally, ICE provides CBP with information on individuals who have exited the country through deportation which is then stored in IDENT and ADIS.

inadvertently reported that individuals were on board when they were not. CBP officials stated there is ongoing work to identify these issues and improve the match rate by monitoring and reviewing outbound flight data. [29]

ICE agents and officers were unable to tell us how often subjects of investigation were incorrectly recorded as having left the country. Such false departure information resulted in ERO officers closing visa overstay investigations of dangerous individuals, such as suspected criminals, who were actually still in the United States and could pose a threat to national security. For example, an ERO officer stated that a suspect under investigation was listed as having left the country, but had given his ticket to a family member and was still residing in the United States.

Recommendations

Recommendation 4: We recommend the DHS CIO continue to assess current plans to expedite development and implementation of a biometric exit system and ensure continued progress through dedicated reviews, acquisition oversight, and corrective action plans, as appropriate.

Recommendation 5: We recommend the DHS CIO continue its efforts to evaluate the extent to which the data used to develop overstay estimates are accurate and reliable, identify and document any remaining gaps and limitations, and identify how the data may be improved.

Unintegrated Systems and the Lack of an Exit System Resulted in Poor Overstay Reporting and Inefficient Tracking

Given the unintegrated systems and the lack of a biometric departure system, DHS could not account for all visa overstays in its reporting to Congress. Moreover, the use of inefficient systems in the visa tracking process contributed to case backlogs and diverted resources from locating actual overstays that could pose public safety or homeland security risks.

Inability to Ensure Complete Overstay Reporting to Congress

DHS could not ensure it accounted for the total number of overstays in the country in its annual report to Congress, known as the *Entry/Exit Overstay Report*. The report includes data, by country and by certain classes of admission, on overstays by foreign visitors to the United States who were

[29] CBP reported that APIS was over 94 percent accurate at matching flight manifests.

expected to leave by a specified time. DHS completed its first and only overstay report in 2015 and at the time of our audit was working to compile the report for the subsequent year. The 2015 report had been sent to Congress for its oversight purposes and posted on the DHS website for viewing by the general public.[30]

DHS recognized that the number of overstays listed in its 2015 report to Congress did not account for all visa holders who visited the United States. The report listed 527,127 nonimmigrant visitors as overstays, out of approximately 45 million visitors in 2015. However, the report's overstay figure did not include individuals who had traveled to the country on student visas or anyone who crossed the border by land from Canada or Mexico. Because of unreliable collection of departure data at these ports of entry, the Department could not account for these potential overstays. Therefore, the report was limited in that it only included individuals traveling to the United States by air or sea on business travel or tourism.

Further, the Department could not provide assurance that all nonimmigrants who overstayed their period of admission had been caught. DHS' inability to accurately confirm the departures of all nonimmigrants from the United States at the end of their authorized admission periods prohibited ICE agents and officers from fully accomplishing their immigration enforcement and removal responsibilities. To illustrate, ICE agents and officers arrested only 3,402, or less than 0.4 percent, of the people who potentially overstayed their visas in 2015.[31] In some cases, the individuals arrested had been reported in DHS systems as having already left the United States. Because this information was not recorded, ICE personnel were unable to provide an exact number when asked during our audit.

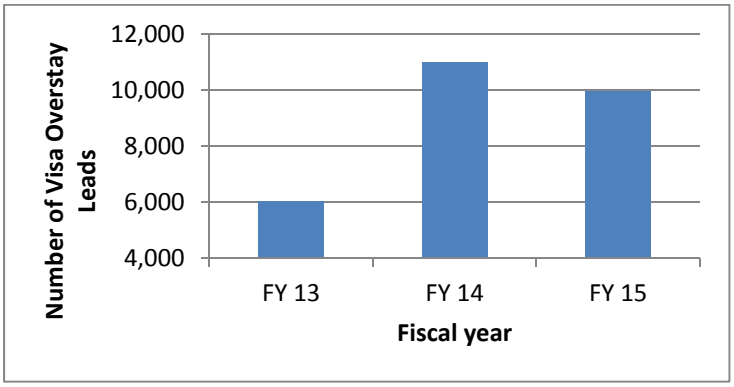
[30] *Entry/Exit Overstay Report,* Fiscal Year 2015, January 19, 2016. https://www.dhs.gov/sites/default/files/publications/FY15DHSEntryandExitOverstayReport.pdf
[31] Of the 971,305 leads sent to CTCEU that were not closed through automated vetting or manual closure, 3,402 arrests were made. Of the total 3,402 individuals arrested, 777 were cases sent to the field in previous fiscal years.

Inefficient Use of Time and Effort to Track Visa Overstays

Given the inefficient systems and management processes, visa overstay tracking is a laborious process. It can take months for HSI personnel to make a determination on whether a subject legitimately overstayed a visa and send the case to the field for further investigation to conclude whether he or she was deemed a risk to public safety or national security. Although HSI agents utilized a triage approach to investigate highest priority cases first, the labor-intensive process of researching and cross-checking numerous data sources slowed visa tracking operations. HSI field personnel stated they routinely spend a significant amount of time, several days in some instances, to manually extract and compile data to support a decision on whether to actively pursue a potential overstay. Working in this manner contributed to the inability of CTCEU to address and close a backlog of more than 1.2 million cases that were in continuous monitoring from previous fiscal years as well as FY 2015.[32]

Amid the backlog, HSI agents in the field have experienced increases in their workloads as the number of overstay leads has increased by 65 percent over the last 3 years (see figure 5). Specifically, the number of leads that CTCEU sent to HSI agents in the field increased from 6,033 in FY 2013 to 9,968 in FY 2015. Without better IT systems, ICE will continue to face inefficiencies and backlogs in overstay investigation cases that otherwise might have been avoided.

Figure 5: Number of Overstay Leads Sent to HSI from FY 2013 to FY 2015



Source: OIG-generated based on DHS data

Furthermore, ICE personnel lost a significant amount of time investigating individuals who should not have been considered overstays. The diversion of

[32] CTCEU reportedly conducts continuous monitoring as part of its investigative work, which includes checking social media and doing manual reviews for individuals with incomplete information and juveniles.

time and effort prohibited ICE personnel from locating actual overstays who potentially posed public safety or homeland security risks. To illustrate, CTCEU HSI analysts and agents spent significant time working on open cases during FY 2015. However, more than 40 percent of the cases sent to HSI agents in the field were closed because the individuals had departed the country or had applied for or received immigration benefits, such as a visa extension, to extend their time in the United States (see table 3).

Table 3: Percentage of HSI Investigations that Were Not Overstays

Potential Overstays Sent to HSI Agents in the Field	Number	Percent of total leads*
Nonimmigrants who were not actual visa overstays	4,148	42%
-- Those who had departed the country	*1,649*	*17%*
--Those who had applied for/received USCIS Benefits	*2,499*	*25%*
Nonimmigrants who were actual visa overstays	5,820	58%
Total vetted overstay suspects sent for investigation	**9,968**	**100%**

Source: OIG-generated based on DHS data

As table 3 shows, approximately 17 percent, or 1,649 of 9,968 overstay leads sent to HSI field agents for investigation in FY 2015 were closed because the subjects had already departed the country. In one case, an HSI agent found that 9 of his 48 leads closed in FY 2015 were for investigating subjects who had already exited. The agent estimated these 9 leads consumed a total of 225 investigative hours. In a second case, an HSI agent reportedly spent 2 months searching for an individual listed as still in the country, only to find that the subject had departed the prior year. In a third case, an HSI agent had ICE headquarters remove 73 leads from his caseload in FY 2015 after determining the suspects had departed the country; 15 of them had left the year before.

Further, table 3 shows that 25 percent, or 2,499, of the overstay cases referred to HSI field agents for investigation in FY 2015 had applied for, or had been approved for, immigration benefits. In one case, an HSI agent had ICE headquarters remove 53 suspects from his caseload after determining that they had applied to USCIS for visa extensions or immigration benefits. In a second case, an ICE officer estimated that he spent more than 50 hours on a single suspect, only to find the individual had applied for a USCIS benefit and should not have been categorized as an overstay. In a third instance, an HSI agent spent 9 days checking databases, making site visits, and conducting interviews to search for an overstay suspect who had applied for permanent residence after marrying a U.S. citizen, which made the subject automatically eligible to stay in the country.

The time wasted on investigating false leads increased the risk that legitimate overstays were being overlooked. In some instances, overstay suspects committed crimes while ICE agents remained mired in the inefficient overstay tracking process. To illustrate, one ERO officer stated that a suspect committed crimes, including domestic abuse and drug-related offenses, while the officer waited for the suspect's immigration files to arrive from USCIS. In another example, an HSI agent's pursuit of an overstay suspected of narco-terrorism activities was delayed for at least 6 months while the agent waited for a file from USCIS. Further, ICE officials were concerned that while time was spent on individuals who had departed or lawfully remained in country, others who actually posed public safety or homeland security risks could go undetected or uninvestigated in a timely manner.

OIG Analysis of Management Comments

We obtained written comments on a draft of this report from the Director of the Departmental GAO-OIG Liaison Office. We have included a copy of the comments in their entirety in appendix B.

In the comments, DHS concurred with our recommendations and provided details on the Department's progress in addressing potential security risks created by visitors who remain in the United States after their period of admission has expired. Specifically, DHS mentioned recent efforts to draft the FY 2016 overstay report, which will include more than 97 percent of all nonimmigrants admitted by air and sea to the United States during the fiscal year. DHS also included information on progress made toward implementing a biometric exit solution and highlighted its recent facial recognition pilot effort conducted during FY 2016. We reviewed these comments and have provided our evaluation below.

Recommendation 1: We recommend the DHS CIO continue to work with components to further eliminate duplication, improve information sharing, and properly align system access, especially for system modernization efforts, across DHS according to visa tracking mission requirements.

Management Comments

In response to recommendation 1, the CIO concurred, stating that as systems are modernized the DHS Office of the CIO will help identify potential gaps in services resulting from changes to component programs. The Office of the CIO indicated that its involvement will help ensure system users are provided with the information they need across components as modernization efforts

continue. The CIO estimated that these actions would be completed by October 31, 2017.

OIG Analysis

We agree that the DHS CIO's continued involvement in system modernization efforts will help to identify gaps in service and ensure that appropriate access to necessary information is granted to ICE personnel. We look forward to receiving further updates on how these efforts may lead to improved system integration and access. This recommendation is open and resolved.

Recommendation 2: We recommend that the ICE CIO assess and address the visa IT training needs of ICE users, including coordinating with system owners in other components to ensure that ICE users have the opportunity to receive official, hands-on training on these components' visa IT systems as well.

Management Comments

Responding to recommendation 2, the ICE CIO concurred, and outlined a plan to identify and address training gaps for ICE personnel. The ICE CIO's plan included collaborating with HSI and ERO to identify training gaps, working with internal and external DHS partners to identify training points of contact for systems used for overstay tracking, and outreach to ensure training options are available to system users. The ICE CIO anticipated that these actions would be completed by April 30, 2018.

OIG Analysis

We agree with the ICE CIO's approach to develop a plan to identify and address training gaps for visa-related IT systems used by ICE personnel. We look forward to receiving further updates as this plan is implemented. This recommendation is open and resolved.

Recommendation 3: We recommend that the ICE CIO compile an up-to-date inventory of all IT systems across the Department that ICE agents and officers can use for visa tracking and provide documented guidance on potential uses of each system to accomplish the various visa overstay tracking responsibilities.

Management Comments

The ICE CIO concurred with recommendation 3 and stated that the ICE Office of the CIO will complete a comprehensive list of all visa-related systems across

the Department, including system owners and training points of contact, and distribute the information to ICE system users. The CIO estimated that these actions will be completed by April 30, 2018.

OIG Analysis

We agree with the ICE Office of the CIO's efforts to complete a comprehensive list of all visa related systems across the Department. We look forward to receiving updates as this list is developed and distributed to ICE system users. This recommendation is open and resolved.

Recommendation 4: We recommend the DHS CIO continue to assess current plans to expedite development and implementation of a biometric exit system and ensure continued progress through dedicated reviews, acquisition oversight, and corrective action plans, as appropriate.

Management Comments

The DHS CIO concurred with recommendation 4, agreeing with the need for a biometric exit capability to be deployed in an expeditious manner. The CIO stated that the Office of the CIO will continue to provide governance and support to ensure the biometric exit program is prepared for the Acquisition Lifecycle Framework milestones, and anticipated approval of the biometric exit system's acquisition lifecycle framework gate review by August 30, 2017.

OIG Analysis

We recognize the DHS CIO's ongoing role in providing governance and support for the biometric exit program as part of the Acquisition Lifecycle Framework. We look forward to learning more following the August 30, 2017, acquisition lifecycle framework gate review. This recommendation is open and resolved.

Recommendation 5: We recommend the DHS CIO continue its efforts to evaluate the extent to which the data used to develop overstay estimates are accurate and reliable, identify and document any remaining gaps and limitations, and identify how the data may be improved.

Management Comments

Responding to recommendation 5, the DHS CIO concurred and indicated that the Office of the Chief Information Officer has partnered with Department components to help standardize overstay data. Further, data quality will improve as a result of biometric matching and the closing of information gaps

in land departure reporting. The DHS CIO stated that the Office of the CIO will continue to monitor the program for gaps in data quality, availability, and consistency. The CIO estimated that these actions will be complete by September 30, 2017.

OIG Analysis

We agree with the actions described by the DHS CIO to partner with DHS components to help standardize overstay data and continue to monitor the biometric program for gaps in data quality, availability, and consistency. We look forward to receiving updates once these actions are completed. This recommendation is open and resolved.

Appendix A
Objective, Scope, and Methodology

The DHS Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

As part of our ongoing responsibilities to assess the efficiency, effectiveness, and economy of Departmental programs and operations, we conducted an audit to determine the effectiveness of IT systems to support ICE's ability to review, track, and share information associated with visas.

We researched and reviewed Federal laws, management directives, and agency plans and strategies related to IT systems, management, and governance. We obtained published reports, documents, and news articles regarding ICE's management and use of IT. Additionally, we reviewed recent GAO and DHS OIG reports to identify prior findings and recommendations. We used this information to establish a data collection approach that consisted of focused information-gathering meetings, documentation analysis, site visits, and system demonstrations to accomplish our audit objective.

We held meetings and teleconferences with ICE staff at headquarters and field offices. Collectively, we conducted more than 50 interviews, including meetings with headquarters officials, field office staff, and system users, to learn about ICE IT functions, processes, and capabilities. At headquarters, we met with ICE CTCEU and Office of the CIO representatives, SEVIS program management, OBIM, CBP's Office of Field Operations, National Targeting Center staff, and USCIS Fraud Detection and National Security Directorate personnel. We interviewed ICE Office of the CIO and CBP Office of Information and Technology officials including division directors and program managers to discuss their roles and responsibilities related to ICE IT management. In addition, we met with DHS Office of the CIO staff.

We visited ICE HSI and ERO field locations including New York, NY; Boston, MA; Los Angeles and San Francisco, CA; Houston, TX; and Miami, FL. At ICE field locations, we met with field office directors, HSI agents, ERO officers, task force attachés from the Department of State and USCIS, and other system users to understand IT development practices, user requirements, and system use in the field. We discussed the existing IT environment, the extent to which it supported mission needs, and user involvement and communication with headquarters. We collected supporting documents about the ICE IT

environment, IT systems, and other current initiatives and technology related improvement initiatives.

We conducted this performance audit between May 2016 and September 2016 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix B
Management Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 14, 2017

MEMORANDUM FOR: Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits

FROM: Jim H. Crumpacker, CIA, CPA
Director
Departmental GAO-OIG Liaison Office

SUBJECT: Management's Response to OIG Draft Report: "DHS Tracking of Visa Overstays is Hindered by Insufficient Technology" (Project No. 16-050-ITA-CBP, ICE)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

The Department has made progress in its ability to identify and apprehend individuals trying to illegally enter the United States. This includes effort to address potential security risks created by those individuals who stay beyond the expiration of their visa. For example, the establishment of the Enhance Biographic Exit and Overstay Working Groups and the Exchange Visitor Information System will improve DHS's ability to identify and determine potential threats to our national security and public safety.

Additionally, recent efforts associated with Biometric Exit and the enhancements implemented by U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) have helped modernize the identification and enforcement of non-immigrant overstays. DHS remains committed to improving its capability to implement biometric exit and land border exit solutions that will resolve information gaps associated with entry/exit reporting and overstay enforcement. As part of this process, CBP and others are reviewing the President's "Executive Order: Protecting The Nation From Foreign Terrorist Entry Into The United States," dated January 27, 2017, to determine how best DHS can comply with a requirement to expedite the completion and implementation of a biometric entry-exit tracking system for all travelers to the United States, as recommended by the National Commission on Terrorist Attacks Upon the United States.

It is also important to note, in addition to the aforementioned efforts and others highlighted in the OIG's draft report, CBP has drafted and will soon release an overstay report for fiscal year (FY) 2016, covering nonimmigrant travelers who were expected to depart the United States between October 1, 2015 and September 30, 2016. The report will address more than 97% of all nonimmigrants admitted by air and sea to the United States during FY 2016. It will include overstay rates by country for nonimmigrant Visa Waiver Program (VWP) and B-1/B-2 visa categories. CBP deployed enhanced operational capabilities with ICE to add student (F, M and J) visa categories, along with other nonimmigrant categories, with overstay rates by country. Moving forward, DHS plans to report these numbers on an annual basis. CBP successfully implemented Out of Country Overstay enforcement operations in June 2016 to assist ICE with its overstay enforcement mission. Out of Country enforcement operations have contributed to enforcement of VWP compliance, cancellation of visas, and applicable travel bans of 3 and 10 years for significant overstay violations.

CBP has also made considerable progress with implementing an operational Biometric Exit solution. The facial recognition biometric pilot, conducted at Hartsfield-Jackson International Airport in Atlanta, GA during FY 2016, has provided a blueprint for implementing biometric exit controls. In December 2016, the pilot became the Biometric Verification System (BVS). Using BVS, CBP is now biometrically confirming selected travelers departing the U.S. at Atlanta's international airport. CBP will continue to test different facial image capture devices and work with airlines to more fully integrate BVS into the airline boarding process at additional locations. CBP is committed to progressing other efforts associated with enhanced exit capabilities and will lead DHS efforts to integrate biometric exit technology and processes for travelers departing the U.S.

The draft report contained five recommendations with which the Department concurs. Attached find our detailed response to each recommendation.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Attachment: DHS Management Response to Recommendations Contained in Project No. 16-050-ITA-CBP, ICE

The OIG recommended that the DHS Chief Information Officer (CIO):

Recommendation 1: Continue to work with components to further eliminate duplication, improve information sharing, and properly align system access, especially for system modernization efforts, across DHS according to overstay tracking mission requirements.

Response: Concur. The DHS Office of the Chief Information Officer (OCIO) will continue to be a trusted partner with biometric exit and other related programs. Specifically, as systems are modernized, DHS OCIO will help to identify potential gaps in services resulting from changes to Component programs. DHS OCIO involvement will continue to help ensure users are provided with access to information they need across Components as the Department migrates from the ICE TECS Mod legacy systems and implements the non-immigrant search for Homeland Security Investigations (HSI) users as part of the Student and Exchange Visitor Information System (SEVIS) non-immigrant information module. Estimated Completion Date (ECD): October 31, 2017.

The OIG recommended that the ICE CIO:

Recommendation 2: Assess and address the visa IT training needs of ICE users, including coordinating with system owners in other components to ensure that ICE users have the opportunity to receive official, hands-on training on these components' visa IT systems as well.

Response: Concur. In collaboration with HSI and Enforcement and Removal Operations (ERO), the ICE CIO will identify current training gaps and notify the ICE user community of available training options. The ICE CIO will work with DHS partners to identify system owners and training points of contact (POCs) for those Information Technology (IT) systems, both internal and external to DHS, that support the tracking and enforcement of visa overstays. The ICE CIO will develop training strategies and an outreach program to ensure all users of these IT systems have access to the available training. ECD: April 30, 2018.

Recommendation 3: Compile an up-to-date inventory of all IT systems across the Department that ICE agents and officers can use for visa tracking and provide documented guidance on potential uses of each system to accomplish the various visa overstay tracking responsibilities.

Response: Concur. The ICE OCIO will capture an up-to-date, comprehensive list of all visa-related IT systems across the Department, while identifying system owners and appropriate training POCs and documenting system capabilities relating to visa tracking and enforcement. In

3

collaboration with HSI and ERO, the ICE CIO will distribute the information to the ICE user community. ICE CIO will engage with DHS and external visa IT system owners to encourage full support of additional ICE training requirements and work with all users to ensure they are taking appropriate actions to receive all available training. ECD: April 30, 2018.

The OIG recommended that the DHS CIO:

Recommendation 4: Continue to assess current plans to expedite development and implementation of a biometric exit system and ensure continued progress through dedicated reviews, acquisition oversight, and corrective action plans, as appropriate.

Response: Concur. The DHS OCIO recognizes the need for a biometric exit capability to be deployed in an expeditious manner. In accordance with FITARA and other authorities, DHS OCIO will continue to provide governance and support to ensure that the biometric exit program is prepared for Acquisition Lifecycle Framework (ALF) milestones and any issues will be resolved as quickly as possible, while maintaining due diligence for long term planning. DHS OCIO anticipates the approval of the Biometric Exit program's ALF gate review during the Acquisition Review Board 2B. ECD: August 30, 2017.

Recommendation 5: Continue its efforts to evaluate the extent to which the data used to develop overstay estimates are accurate and reliable, identify and document any remaining gaps and limitations, and identify how the data may be improved.

Response: Concur. The DHS OCIO has partnered with Components to help establish clear data exchange profiles and other artifacts to help standardize overstay data. Use of biometric matching and closing information gaps in land exit reporting should greatly increase the quality of overstay data, and DHS OCIO will continue to monitor the program for gaps in data quality, availability and consistency as that information is integrated. DHS OCIO anticipates the review and approval of the Biometric Exit program's data model and associated migration plans. ECD: September 30, 2017.

4

Appendix C
IT Systems Used for Visa Tracking by ICE Headquarters and Field Personnel

System	Owner	Description
Advance Passenger Information System (APIS)	CBP	Receives passenger and crew biographic data from commercial air and sea carriers prior to arrival or departure from the United States for screening purposes.
Analytical Framework for Intelligence	CBP	Aggregates and indexes data from a variety of DHS source systems to facilitate intelligence gathering and assists users in building intelligence profiles.
Arrival and Departure Information System (ADIS)	CBP	Stores biographic information of travelers entering and departing ports of entry and is the primary means of identifying visa overstays.
Automated Targeting System-Passenger (ATS-P)	CBP	Supports CBP border screening and DOS visa adjudication by providing users with national security vetting results and recommendations for individuals seeking entry to the United States.
TECS Modernization	CBP	Used to perform border screening of people and goods seeking entrance to the United States.
Unified Passenger (UPAX)	CBP	Aggregates data in a consolidated, automated interface to provide continuous vetting of foreign nationals from application through the duration of their visa.
GangNet (Cal/Gang ®)	Commercial (CSRA)	Stores profiles of suspected gang members and allows law enforcement to collaborate and share data on gang activities, their members, and affiliates.
Consolidated Lead Evaluation and Reporting	Commercial (Thomson Reuters)	Maintains data on individuals and companies in a searchable database from a variety of public and private sources.
Consular Consolidated Database Indices	DOS	Maintains current and archived data from all international U.S. consular posts, including immigrant and nonimmigrant visa applications, U.S. passport information, and outside information from the Social Security Administration.
National Crime Information Center	FBI	Houses the FBI's criminal data, such as suspected terrorists lists and criminal histories, and can be queried by law enforcement agencies nationwide.
Enforcement Integrated Database for Law Enforcement	ICE	Serves as booking application system for ERO agents to enter subject details when making an arrest.

System	Owner	Description
ENFORCE Alien Removal Module	ICE	Maintains information on deportation and removal records that is used for case management purposes by ICE ERO personnel.
Enforce Integrated Database	ICE	Provides a centralized platform of law enforcement systems that can search across multiple data sources and case management modules.
FALCON Search and Analysis System (ICE implementation of Palantir)	ICE	Aggregates and analyzes historical data from DHS systems and databases on individuals previously encountered during DHS investigations.
LeadTrac	ICE	Receives visa overstay leads for national security or public safety threats and gathers information on the subjects in a case management system.
Pre-Adjudicated Threat Recognition Intelligence Operations Team	ICE	Receives and vets visa applications from State Department consular posts for admissibility against derogatory information from a variety of law enforcement databases.
Student And Exchange Visitor Information System (SEVIS)	ICE	Receives, tracks, and shares biographic and immigration data on approved educational institutions, exchange visitor programs, and nonimmigrant students and visitors to monitor and report on visa holders' status and compliance.
Investigative Case Management (ICE TECS Modernization)	ICE	Aggregates information from law enforcement databases, facilitates sharing among various Government agencies, and serves as a case management tool for HSI personnel.
Automated Biometric Identification System (IDENT)	NPPD - OBIM	Receives, matches, stores and shares biometric data in an interface used by DHS components to correlate identifying biometric data with associated biographic data.
Secondary Inspection Tool	NPPD-OBIM	Supplements entry/exit screening by cross-referencing an individual's biometric information with the biographic and biometric information previously captured during the immigration or visa process.
National Law Enforcement Telecommunications System	State-owned and operated	Transmits law enforcement information and notices in a messaging system to facilitate information sharing among state and local law enforcement agencies.
Alien Change of Address Request Database	USCIS	Maintains records of foreign nationals' petitions for change of address in a database.
Central Index System	USCIS	Houses historical data on individuals applying for immigrant and nonimmigrant benefits and status, including violators of immigration law.

System	Owner	Description
Computer Linked Application Information Management System 3.0 (CLAIMS 3)	USCIS	Maintains data and supports the end-to-end adjudication process for applications and petitions related to immigration.
Computer Linked Application Information Management System 4.0 (CLAIMS 4)	USCIS	Maintains data and supports the end-to-end adjudication process for applications for naturalization.
Customer Profile Management System	USCIS	Is a repository of USCIS biometric and biographic data on applicants for immigration benefits.
Enterprise Document Management System	USCIS	Contains records of digitized paper A-File that can be searched by law enforcement.
Fraud Detection and National Security Data System	USCIS	Records, tracks, and shares information associated with immigration-related fraud or national security cases, and is the primary case management tool for USCIS' Fraud Detection and National Security directorate.
National Appointment Scheduling System/InfoPass	USCIS	Records and tracks appointments across USCIS, including individuals applying for immigration benefits.
National File Tracking System	USCIS	Maintains record of the physical location of an A-File.
Person Centric Query Service	USCIS	Queries multiple USCIS data systems and returns aggregated results.
Refugees, Asylum And Parole System (RAPS)	USCIS	Maintains and tracks refugee and asylum data, including applications and interview appointments; administers benefits; and generates data used for reporting purposes and national security referral cases from a single database.

Source: OIG-generated from DHS data

Appendix D
Office of IT Audits Major Contributors to This Report

Kristen Bernard, Division Director
Craig Adelman, Audit Manager
Anna Hamlin, Senior Program Analyst
Theresa Lowell, Program Analyst
David Bunning, Referencer

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Acting Director, Office of Biometric Identity Management, National Protection and Programs Directorate
Acting Director, Service Center Operations, U.S. Citizenship and Immigration Services
Acting Assistant Commissioner, Office of Information Technology, Customs and Border Protection
Immigration and Customs Enforcement Audit Liaison
National Protection and Programs Directorate Audit Liaison
U.S. Citizenship and Immigration Services Audit Liaison
Customs and Border Protection Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305