Department of Homeland Security
Office of Inspector General

Information Sharing On Foreign Nationals: Overseas Screening (Redacted)

OIG-11-68

April 2011
(Revised)

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

Homeland
Security

April 7, 2011

Preface

The Department of Homeland Security (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.

This report addresses the strengths and weaknesses of DHS information sharing on foreign nationals overseas. It is based on interviews with employees and officials of relevant agencies, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Charles K. Edwards

Charles K. Edwards
Acting Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

ADIS	Arrival and Departure Information System
APIS	Advance Passenger Information System
ATS-P	Automated Targeting System – Passenger
ATT	Advance Targeting Team
BASS	Biometrics-at-Sea System
CBP	U.S. Customs and Border Protection
CDC	Centers for Disease Control and Prevention
CIO	Chief Information Officer
CIS	Central Index System
CLAIMS3	Computer-Linked Application Information Management System 3
CLAIMS4	Computer-Linked Application Information Management System 4
DHS	Department of Homeland Security
EARM	Enforce Alien Removal Module
ENFORCE	Immigration Enforcement Operational Records System
ESTA	Electronic System for Travel Authorization
FBI	Department of Justice Federal Bureau of Investigation
FLETC	Federal Law Enforcement Training Center
FY	Fiscal Year
HRM	Human Resources Management
HSIN	Homeland Security Information Network
IAP	Immigration Advisory Program
ICE	U.S. Immigration and Customs Enforcement
ICE-PIC	ICE Pattern Analysis and Information Collection System
IDENT	Automated Biometric Identification System
ISRS	Image Storage and Retrieval System
NTC-P	National Targeting Center - Passenger
OIG	Office of Inspector General
PNR	Passenger Name Record
RAPS	Refugees, Asylum, and Parole System
SEVIS	Student and Exchange Visitor Information System
TDY	Temporary Duty
TECS	TECS (not an acronym)
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TWIC	Transportation Worker Identification Credential
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
VWP	Visa Waiver Program

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

The Department of Homeland Security has implemented several programs to screen foreign nationals while they are still overseas. These programs rely on biographical, biometric, and documentary information in the department's and other federal data systems. We evaluated whether levels of cooperation, resources, and technology were adequate for department officers to assess the risks posed by foreign nationals who seek to enter the United States. We also reviewed plans to consolidate and improve information in the department's data systems.

The department has made progress in evaluating admissibility of foreign nationals before they travel to the United States. The level of cooperation among components that conduct overseas screening is high. Headquarters support offices have long-term plans to streamline access to information in the department's data systems, and improve screening and data analysis capabilities.

However, Department of Homeland Security initiatives face serious resource and technological challenges. Information is fragmented among more than 17 data systems, and officers must conduct labor-intensive, system-by-system checks to verify or eliminate each possible match to terrorist watch lists and other derogatory information. The U.S. Customs and Border Protection National Targeting Center – Passenger is the operational core of the department's overseas screening efforts. The center is challenged by insufficient staff and difficult working conditions. Effective small-scale screening and interdiction programs need sufficient resources to meet operational needs and congressional mandates. We are making 18 recommendations to standardize the technology used to share information in departmental data systems, enable federal officers to obtain and use the most current and complete data available, and improve information sharing procedures. Departmental components concurred with 17 of the 18 recommendations. However, for five recommendations with which components concurred, including three that would increase productivity for thousands of DHS employees, components said that they would need to request additional resources in the next federal budget cycle to implement the recommendations.

Background

On December 25, 2009, Umar Farouk Abdulmutallab, a Nigerian national, presented a valid U.S. visa to Dutch authorities and boarded Northwest Flight 253 from Amsterdam to Detroit. Abdulmutallab was not on the Terrorist Screening Database (TSDB) no fly or selectee lists, and was permitted to board. However, officers in Detroit were directed to conduct further screening on arrival because U.S. Customs and Border Protection (CBP) noted en route derogatory information that had been transmitted from the State Department to its data systems.[1] During the flight, Abdulmutallab attempted to detonate explosives carried on his person. The size and complexity of the Department of Homeland Security (DHS) preflight screening program expanded in response to the December 2009 bombing attempt, with more scrutiny of travelers and upgraded preflight screening software.

The capability of DHS to identify and prevent threats depends on technologies that can access and evaluate information rapidly. DHS recognized the importance of accurate and timely information sharing well before these incidents occurred. On February 1, 2007, the DHS Secretary instructed DHS components to give "the highest priority to the sharing of potential terrorism, homeland security, law enforcement, and related information" and to "standardize the technology used to describe, access, exchange, and manage information in our automated systems."[2] On July 2, 2009, the White House reiterated this message in a memorandum to all Cabinet-level federal agencies, and said that achieving "effective information sharing and access" was a top priority. The memorandum noted that "[s]ignificant progress has been made in recent years. … But there is more work to be done."[3]

This report focuses on only one aspect of information sharing: DHS efforts to screen foreign nationals while they are still overseas. We will review other facets of information sharing on foreign nationals, specifically border security and domestic programs, in separate reports. However, this report discusses some

[1] Statement of Janet A. Napolitano, Secretary, United States Department of Homeland Security, United States Senate Committee on Homeland Security and Governmental Affairs, January 20, 2010.

[2] Memorandum from DHS Secretary Michael A. Chertoff to All Department of Homeland Security Components, *DHS Policy for Internal Information Exchange and Sharing*, February 1, 2007.

[3] Memorandum from John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, to cabinet level officials, *Strengthening Information Sharing And Access*, July 2, 2009.

more general issues related to DHS data systems. Addressing these issues may improve information sharing in areas beyond the screening of foreign nationals while they are overseas.

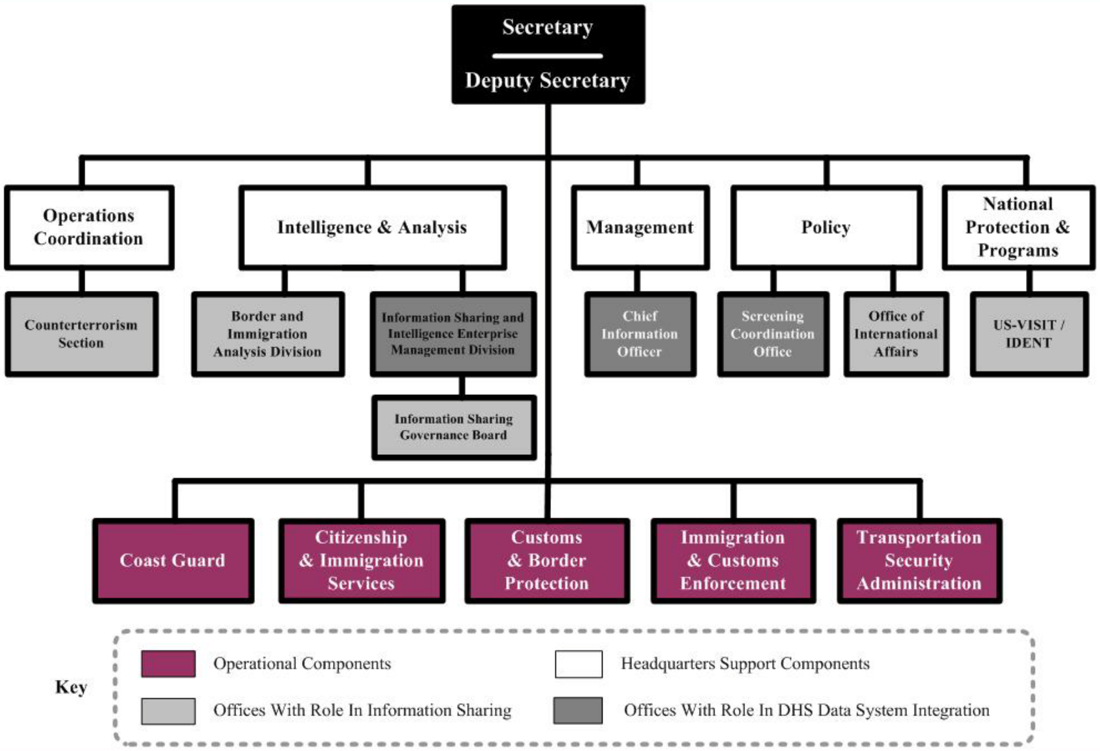
Information sharing within DHS on foreign nationals is the responsibility of five of the seven major DHS operational components, as well as support offices. (See Figure 1.) The operational components are CBP, U.S. Citizenship and Immigration Services (USCIS), U.S. Coast Guard (USCG), U.S. Immigration and Customs Enforcement (ICE), and Transportation Security Administration (TSA), each of which is actively involved in sharing information throughout DHS and with other federal, state, local, and tribal partners. There are four support offices with a role in information sharing:

- The Counterterrorism Section in the Office of Operations Coordination and Planning;
- The Office of Policy, which includes the Screening Coordination Office, the Office of International Affairs and the Office of Policy Development;
- The Border and Immigration Analysis Division in the Office of Intelligence and Analysis; and
- The U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program in the National Protection and Programs Directorate.

In addition, there are two support offices with a role in DHS data systems integration:

- The Information Sharing Intelligence Enterprise Management Division in the Office of Intelligence and Analysis; and
- The Office of Chief Information Officer in the Office of Management.

Figure 1: DHS Components Responsible for Information Sharing on Foreign Nationals


Secretary
Deputy Secretary
Operations Coordination
Intelligence & Analysis
Management
Policy
National Protection & Programs
Counterterrorism Section
Border and Immigration Analysis Division
Information Sharing and Intelligence Enterprise Management Division
Chief Information Officer
Screening Coordination Office
Office of International Affairs
US-VISIT / IDENT
Information Sharing Governance Board
Coast Guard
Citizenship & Immigration Services
Customs & Border Protection
Immigration & Customs Enforcement
Transportation Security Administration
Key
Operational Components
Headquarters Support Components
Offices With Role In Information Sharing
Offices With Role In DHS Data System Integration

Source: Office of Inspector General (OIG)

In the past decade, the U.S. government has expanded its legal authority to screen foreign nationals while they are overseas. This authority allows the State Department and DHS to collect and share biographical, biometric, and documentary information on foreign nationals who apply for a visa or seek to travel to the United States. Legal authorities for sharing information on foreign nationals are listed in Appendix C, and include the following:

- *Aviation and Transportation Security Act of 2001*: adds mandatory manifest and passenger name record and other aviation screening requirements.[4]
- *Enhanced Border Security and Visa Entry Reform Act of 2002*: requires biometric-based visas and travel documents, electronic transmission of passenger manifests, and DHS tracking of foreign students.[5]

[4] P.L. 107-71.

[5] P.L. 107-173.

- *Homeland Security Act of 2002*: provides the DHS Secretary authority to access all information related to threats against the United States, and to assign DHS officers to high-risk consulates to review visas.[6]
- *Intelligence Reform and Terrorism Prevention Act of 2004*: requires in-person interviews for most visas, Immigration Advisory Program officers to be located at foreign airports, integration of DHS and other federal data systems, and DHS control of preflight watch list screenings (Secure Flight).[7]
- *Implementing Recommendations of the 9/11 Commission Act of 2007*: requires Visa Waiver Program countries to share information on threats and on lost and stolen passports. Applicants from a Visa Waiver Program country must obtain an Electronic System for Travel Authorization (ESTA) approval before they travel to the United States.[8]

DHS screening programs require access to information collected and maintained in a range of databases and data systems. These include databases from other federal agencies, for example:

- The Department of State, which tracks information on visa applicants;
- The Department of Justice Federal Bureau of Investigation (FBI), which tracks known and suspected terrorists and known criminals, also leads the interagency Terrorist Screening Center (TSC), which maintains the consolidated TSDB watch list of known and suspected terrorists; and
- The Centers for Disease Control and Prevention (CDC), which tracks individuals with diseases that would pose a serious health threat to fellow air travelers.

Screening programs also include DHS data systems, ranging from systems developed in the 1980s to modern specialized single-purpose systems, which manage information on specific categories of foreign nationals, such as students and Visa Waiver Program applicants. We identified 17 major DHS data systems that manage information on international travel and the status of foreign nationals. Systems that manage information on international travel include both U.S. citizens and foreign nationals. Systems that manage information on foreign nationals can include individuals who have obtained, or could in the future obtain, lawful

[6] P.L. 107-296.

[7] P.L. 108-458.

[8] P.L. 110-53.

permanent resident status, or citizenship through naturalization. (See Figure 2 and Appendix E.)

Figure 2: DHS Systems For Travel And Immigration Screening

	DHS INFORMATION SYSTEMS
Owner	**Manages Information On Foreign Nationals (who may become US citizens)**
US-VISIT	**ADIS**
➢	Arrival and Departure Information System
➢	Collects, matches, and reports on U.S. arrivals and departures
USCIS	**CIS**
➢	Central Index System
➢	Documents status of applicants/petitioners seeking immigration benefits
USCIS	**CLAIMS3**
➢	Computer-Linked Application Information Management System 3
➢	Tracks immigrant and nonimmigrant applications / petitions
USCIS	**CLAIMS4**
➢	Computer-Linked Application Information Management System 4
➢	Tracks naturalization applications
ICE	**EARM**
➢	Enforce Alien Removal Module
➢	Tracks detained aliens, aliens in removal proceedings, and case histories
ICE	**ENFORCE**
➢	Immigration Enforcement Operational Records System
➢	Tracks immigration enforcement actions and cases
CBP	**ESTA**
➢	Electronic System for Travel Authorization
➢	Screening mechanism for applications from visa waiver travelers for travel authorization
US-VISIT	**IDENT**
➢	US-VISIT Automated Biometric Identification System
➢	Enrolls and stores biometrics of foreign nationals
USCIS	**ISRS**
➢	Image Storage and Retrieval System
➢	Provides query and retrieval of biometric image sets, biographical data
USCIS	**RAPS**
➢	Refugees, Asylum, and Parole System
➢	Tracks affirmative applicants for asylum status
ICE	**SEVIS**
➢	Student and Exchange Visitor Information System
➢	Tracks and monitors students, exchange visitors, and dependents
	Manages Information on Travelers (including US citizens)
CBP	**APIS**
➢	Advance Passenger Information System
➢	Transmits air and sea passenger manifests
TSA	**Secure Flight**
➢	Secure Flight
➢	Watch list matching for flights into, out of, within, and over the United States
	Aggregates / Analyzes Information
CBP	**ATS-P**
➢	Automated Targeting System – Passenger
➢	Provides an enforcement and decision support tool
ICE	**ICE PIC**
➢	ICE Pattern Analysis and Information Collection System
➢	Provides an information analysis tool
ICE	**Intel Fusion / Avalanche**
➢	Intel Fusion / Avalanche / Virtual Investigative & Intelligence System
➢	Provides access to TECS, ENFORCE, encounters, and arrests
	Manages Law Enforcement Information (including US citizens)
CBP	**TECS**
➢	TECS (not an acronym)
➢	Collects, analyzes, and shares law enforcement information

Source: Database documentation, demonstrations

DHS Screens Air And Sea Passengers Pre-departure

DHS initiates extensive screening of airline passengers before they board, and the process continues while they are en route to the United States. Screening is conducted with information passengers provide as they make reservations, purchase tickets, and check in for travel. Screening is also conducted on flight crews, including cargo flights. Figure 3 lists the minimum information that must be provided to DHS and the deadlines to provide the information for air travel.

During the period of our review, Secure Flight was operational and had begun deploying to U.S. aircraft operators and foreign air carriers. As of June 22, 2010, Secure Flight completed deployment for all U.S. aircraft operators' domestic and international flights. As of November 23, 2010, Secure Flight completed deployment to all covered foreign air carriers originally scheduled for implementation. Secure Flight requires airlines to collect and submit passengers' full name (as it appears on the government-issued identification they plan to use when traveling), date of birth, gender, and, if available, a Redress Number for travelers whose names are a false positive match to information on the TSDB watch list. For reservations made prior to 72 hours before departure, aircraft operators are required to transmit Secure Flight Passenger Data to TSA at approximately 72 hours before departure time. For reservations made within 72 hours of departure time, aircraft operators are required to submit Secure Flight Passenger Data as soon as the reservation is made. Secure Flight is designed to perform real-time matching for all flights, including next-day or same-day flights. Based on the results of the watch list matching process, cleared passengers will be able to receive a boarding pass. If a passenger is identified as a Selectee, they will receive a boarding pass that designates them for enhanced screening at the security checkpoint prior to boarding the aircraft. If the aircraft operator receives an "Inhibited" response for a passenger, the aircraft operator cannot issue a boarding pass for that passenger to board the aircraft and TSA will facilitate the notification of the appropriate law enforcement authorities.[9]

The deadlines for submitting advance passenger information depend on the method of transmission. Carriers that do not submit passenger manifests electronically must make a batch submission

[9] 49 CFR Parts 1540, 1544, and 1560, Secure Flight Program; Final Rule, Federal Register, Volume 73, Number 209, Tuesday, October 28, 2008.

of passengers checked in for the flight and receive a non-electronic response from DHS on whether the passengers are cleared. Carriers may, with CBP certification, transmit manifest information electronically through a transmission system configured for batch transmissions and receive an electronic response from DHS systems on whether the passengers are cleared. Both manual and electronic batch submissions must be completed no later than 30 minutes before departure. Carriers may also, with CBP certification, transmit manifest information on individual passengers as they check in for a flight and receive an electronic response from DHS systems on whether each individual passenger has cleared. Information may be sent to CBP via this method, known as Advance Passenger Information System (APIS) Quick Query, until the doors of the aircraft are secured. (See APIS graphic in Appendix E.)

Figure 3: Air Passenger Notification Procedures

Passenger Name Record (PNR)[10]	Advance Passenger Information System (APIS)[11]	Secure Flight (Fully Implemented December 2010)[12]
DHS System Owner	*DHS System Owner*	*DHS System Owner*
➢ CBP	➢ CBP	➢ TSA
May Include	*Must Include*[13]	*Must Include*
➢ Traveler's name Contact details Travel itinerary Reservation details	➢ Traveler's name Date of birth Gender Country of citizenship Travel document number United States address (required only of foreign nationals)	➢ Traveler's name as it appears on a travel document Date of birth Gender Redress Number (if available)
Must Be Provided	*Must Be Provided*[14]	*Must Be Provided*
➢ Up to 72 hours before departure, as available	➢ 30 minutes before the aircraft is secured (batch submissions) Up to securing the aircraft (APIS Quick Query)	➢ Automated, up to 72 hours before departure, or with electronic confirmation (if within 72 hours)

Sources: Statute, regulations, CBP and TSA websites

The CBP National Targeting Center – Passenger (NTC-P) screens lists of all inbound and some outbound international passengers and crew against the terrorist watch list, TSDB, the Centers for Disease Control and Prevention public health "do not board" list, and other information on high risk individuals available in DHS and other federal databases. For flights, when a traveler is identified on a no fly or do not board list, or is inadmissible based on information in a TSDB record or other evidence in DHS systems, CBP officers stationed overseas can assist the airlines in determining a course of action. CBP officers do not have the authority overseas to prohibit travel; however, carriers must comply with no fly and public health do not board cases. Carrier compliance with recommendations against boarding based on inadmissibility is strong, and carriers can be denied landing,

[10] 49 U.S.C. Section 44909(c)(3), 19 CFR Section 122.49d. http://www.cbp.gov/xp/cgov/travel/clearing/pnr/

[11] 8 U.S.C. Section 1221, 19 CFR Section 122.49a (b). http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/apis/

[12] 49 U.S.C. Section 44903(j)(2), 49 CFR Section 1546.101. http://www.tsa.gov/what_we_do/layers/secureflight/

[13] 8 U.S.C. Section 1221, 19 CFR Section 122.49a (b) (3).

[14] 19 CFR Section 122.49a (b)(1) & (2). http://www.cbp.gov/linkhandler/cgov/travel/inspections_carriers_facilities/apis/apis_faqs.ctt/apis_faqs.doc

sanctioned, or fined if necessary. Host government support for U.S. compliance requirements is also strong.

Screening of vessels, including passenger and cargo ships and their crews, is a shared responsibility of CBP and the USCG. Commercial vessel arrival APIS data is required 96 hours before entering the United States at the earliest, and 24 hours before entering the United States at the latest, so passengers may already be on board when APIS information is transmitted and screening begins. The USCG and CBP coordinate in screening passenger and crew manifests of all vessels that are required to provide advance notice of information against the same databases as are used for flights. There is generally more time to screen commercial and cargo vessels than flights, which allows DHS to alert other interested federal partners while the ship is still en route to the U.S.

Information Sharing Drives Visa and Visa Waiver Programs

In addition to CBP and USCG screening programs listed above, there are other DHS programs to assist with screening foreign nationals overseas. Foreign nationals from most countries must obtain a visa from the Department of State to travel to the United States. Visa applicants provide biographical, biometric, and travel document information to consular officers overseas, and are interviewed to evaluate eligibility for a visa. Applicant fingerprints are enrolled in the DHS US-VISIT Automated Biometric Identification System (IDENT), which checks the fingerprints against existing records, and sends an alert if subsequent relevant derogatory information becomes available. When these travelers arrive at a U.S. port of entry, CBP officers check their biometric information for matches to records of known or suspected terrorist, criminals, and immigration violators in DHS and other federal data systems.

There are 36 countries that have visa waiver agreements with the United States (see Appendix D). Each country is subjected to a periodic independent intelligence assessment to maintain eligibility. The Visa Waiver Program allows most nationals from these countries who visit the United States for short-term business or tourism to travel without a visa. Security for the Visa Waiver Program was tightened in 2007, pursuant to the *Implementing Recommendations of the 9/11 Commission Act of 2007*, when participating countries were required to share certain information with the United States. This information includes biographic and some biometric information on known or suspected terrorists and on criminals convicted of felonies that would render them ineligible to enter or remain in the United States. Participating countries must also share information on lost and stolen issued passports, and the passport number for each stolen or missing blank passport. Visa Waiver Program travelers are required to submit their fingerprints and be photographed upon arrival in the United States. Most visa holders enroll in IDENT when they apply for a visa, and on arrival to the United States, their prints are verified.

The *Implementing Recommendations of the 9/11 Commission Act of 2007* required that Visa Waiver Program travelers obtain an electronic travel authorization through the ESTA website. ESTA was introduced in August 2008 and became mandatory in January 2010. ESTA requires applicants to provide biographic and passport information and answer questions about eligibility for admission to the United States, and recommends that such information be submitted at least 72 hours before travel to resolve potential derogatory information.[15] Via ESTA, CBP screens applicants against data contained in law enforcement databases, including TSDB and FBI's database of criminal records, as well as State Department visa revocations, DHS information on visa overstays, and other information in DHS and federal data systems. When there is no potentially derogatory information provided by the applicant or located in the databases, ESTA automatically approves the travel authorization. When the applicant volunteers information on criminal convictions or terrorist activity, the ESTA application is automatically denied. When there is potentially derogatory information on the application or in the data systems that is not conclusive, such as a possible match to watch list information, targeting specialists at the NTC-P evaluate the information against data in other systems to determine whether to authorize travel, and may then either manually approve or deny the application. Based on the Immigration and Nationality Act, commercial air carriers may be fined if they bring passengers with a denied ESTA, or without travel authorization through ESTA. CBP advises passengers and airlines that denials must be resolved through the Department of State.

[15] http://www.cbp.gov/xp/cgov/travel/id_visa/business_pleasure/vwp/faq_vwp.xml

DHS Officers Overseas Assist Screening Foreign Nationals

The most comprehensive overseas screening is CBP's pre-clearance program. Pre-clearance provides a full immigration and customs screening overseas.[16] As appropriate for nationality and visa category, CBP officers in pre-clearance locations enroll travelers' fingerprints in IDENT and can verify whether there is any derogatory information associated with this biometric information. They check DHS and other federal databases for terrorist and other derogatory information, and conduct screening interviews. CBP officers conducting pre-clearance have the same authority as CBP officers at domestic ports of entry to deny entry into the United States, and once pre-cleared, a passenger is admitted to the United States and does not need to be inspected again on arrival. CBP pre-clearance in Canada was established in 1952, and expanded to the Caribbean in 1960. Pre-inspection for immigration was extended to Ireland in 1986, which later received full pre-clearance authorization.[17] Pre-clearance operations are not likely to be expanded widely, as the cost to inspect all travelers overseas is high, and the program requires agreements from host governments and significant reconfiguration of the airline, sea, or rail terminals.

ICE visa security units overseas assist State Department efforts to deny visas to inadmissible foreign nationals and secure the visa issuance process. In accordance with the *Homeland Security Act of 2002*, the Visa Security Program assigns experienced special agents to high-risk consular posts to review visa applications, initiate visa security-related investigations, and provide advice and training to consular officers.[18] In a 2008 report, we concluded that the program "enhances national security by preventing terrorists, criminals, and other ineligible applicants from receiving visas, and maximizing the visa process as a counterterrorism tool."[19] In Fiscal Year (FY) 2009, visa security units screened close to 905,000 visa applicants. Of 301,700 applications that required

[16] http://www.cbp.gov/xp/cgov/toolbox/contacts/preclear_locations.xml

[17] At the time of our review, some locations which were authorized to conduct full pre-clearance, including the Dublin airport and the Vancouver train station, conducted only pre-inspection for immigration. Dublin will introduce full pre-clearance in 2011.

[18] P.L. 107-296, Section 428 (e)(1) and (e)(2).

[19] DHS OIG, *U.S. Immigration and Customs Enforcement Visa Security Program*, OIG-08-79, July 2008, p. 1.

further review, ICE collaborated with Department of State to recommend refusal of more than 1,000 applicants.[20]

Other DHS officers stationed at embassies and consulates use DHS data systems to conduct adjudications or assist in law enforcement investigations. USCIS obtains biographical and biometric information and conducts extensive systems checks for most refugees before they are authorized to travel to the United States. USCIS conducts adjudications on applications for foreign nationals who request immigration benefits outside the United States. These include military naturalizations, adoptions, and petitions for alien relatives. They also include requests for waivers from aliens who have been determined inadmissible for offenses such as minor criminal convictions or visa overstays. USCIS Overseas Verification Program officers in Frankfurt, Germany; Monterrey, Mexico; and New Delhi, India, provide an additional layer of scrutiny for some cases through verification of facts, statements, events, and certain documents that relate to the eligibility of petitioners or applicants to receive immigration benefits from USCIS.

In addition, the Department of State, CBP, ICE, and USCIS share responsibility to assist lawful permanent residents who have lost their documents. If their identity and status can be verified, lawful permanent residents can obtain a transportation letter, which allows them to travel to the United States to replace their permanent resident card. Finally, ICE officers overseas cooperate with host governments to investigate money laundering, human trafficking, and smuggling of aliens, narcotics, or weapons. To assist these investigations, ICE checks whether DHS and other federal data systems have information on the identities and locations of suspected terrorists or criminals.

In addition to pre-clearance operations and DHS officers operating at embassies and consulates, the CBP Immigration Advisory Program (IAP) is a valuable counterterrorism, law enforcement, and facilitation asset for foreign partners and airline stakeholders. The *Intelligence Reform and Terrorism Prevention Act of 2004* called for CBP to identify 50 foreign airports for expansion of the program by December 31, 2006. The process to identify the

[20] Testimony of ICE Assistant Secretary John Morton before the U.S. Senate Committee on Homeland Security and Governmental Affairs, April 21, 2010, available at http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=b5908d92-992b-47b4-a7c0-efa6a663327f

foreign airports has been repeated annually, to reflect changes in travel patterns and threats.[21] Officers have been deployed to 10 foreign airports in eight countries and there are negotiations with foreign governments to deploy IAP to additional locations.[22] Their mission is to intercept high-risk and improperly documented travelers who seek to board a flight to the United States. They work with the NTC-P to identify potential high-risk passengers, and review travel documents and conduct interviews for U.S.-bound travelers. They observe the airport environment to gather information, and exchange it with local security officials. Additionally, officers facilitate legitimate travel. They can assist U.S. citizens and lawful permanent residents who have lost travel documents, or Visa Waiver Program nationals who have made errors on their ESTA applications. In FY 2009, officers recommended 2,776 passengers not board flights for the United States, with cost avoidance for air carriers of $4,535,850, and $4,117,138 for CBP in expenses for secondary inspections at ports of entry. The recommendations against boarding also avoided costs for ICE and Department of Justice immigration judges for detention and removal proceedings.

For ports that do not have a CBP officer present, CBP Regional Carrier Liaison Groups provide assistance. Regional Carrier Liaison Groups in New York, Miami, and Honolulu maintain close ties with airlines that serve Europe and Africa, the Americas, and Asia, respectively. Where there are no CBP officers stationed overseas, the regional CBP liaison can call the airline to obtain more information or recommend against boarding.

USCG migrant interdictions at sea represent another opportunity to prevent unauthorized access to the United States. In most instances the USCG, in consultation with the USCIS Refugee Affairs Division, the State Department, other concerned federal partners, and countries of origin, will repatriate intercepted migrants who are not in need of international protection. However, the USCG has piloted a successful Biometrics-at-Sea System (BASS). BASS confirms the identities of illegal migrants while they are temporarily detained at sea. As the USCG collects a migrant’s information, it is compared to biometric data and the

[21] P.L. 108-458.

[22] The locations are Amsterdam, Netherlands; Warsaw, Poland; London (Heathrow), United Kingdom; London (Gatwick), United Kingdom; Manchester, United Kingdom; Tokyo, Japan; Frankfurt, Germany; Seoul, South Korea; Madrid, Spain; and Paris, France. The Paris, France location was added after completion of our field work.

data matched against information in IDENT. Hand-held biometric devices are used to enroll the fingerprints and transmit them by maritime satellite communications service. Currently, the program is limited to the western coast of Puerto Rico, where Dominicans and a small number of Cubans attempt passage, and a small operation off the southwestern coast of Florida, where the caseload is more varied. Biometric verification has deterred large-scale illegal migration. Between 2007, when the use of biometrics began, and 2009, the USCG collected more than 2,500 biometric enrollments. Of them, about 25% yielded a positive match, and there were approximately 250 successful prosecutions. Interdictions during this period dropped by 75% where biometrics were checked, and the USCG estimated that boat interdictions in these regions might drop from the pre-2006 level of 11,000 to fewer than 1,000 in 2010.

In addition, the USCG is conducting an operational demonstration of biometrics use to reduce security risks from foreign flag liquefied natural gas ships arriving in the United States from regions with elevated terrorist activity. Ship crews are required to have current U.S. visas and are subject to biometric identification. Biometric and biographic information from the ship's manifest and visa records is screened for derogatory information prior to the ship's arrival in U.S. waters. Upon arrival, the ship is boarded to ensure no stowaways or other unknown persons are on board and crewmember identities are verified using fingerprint biometrics. Biometric verification ensures that no individuals known or suspected of association with violent extremism or posing other criminal or security threats are on board.

Results of Review

DHS databases, developed over decades to fulfill a complex range of antiterrorism, law enforcement, immigration, and traveler screening missions, are fragmented. Consolidating most systems is not a practical goal given divergent operational requirements and funding constraints. Cooperation among the operational components that first encounter foreign nationals overseas has helped overcome some of the challenges that DHS data systems present. Short-term improvements can be implemented if DHS expands storage of biometrics in IDENT and improves the ESTA website. More complex planning should take place through the Shared Mission Communities fostered by the Office of Intelligence and Analysis Information Sharing Governance Board.

The NTC-P is the operational core of DHS antiterrorism passenger screening efforts for air and land borders, and partners with the USCG on screening maritime borders. Its responsibilities and workload have increased substantially in response to border security threats. CBP officers often must respond to a potential threat within 30 minutes before a flight departs; however, fragmented DHS data systems make assessing passengers a labor-intensive process. Serious staff shortages, extensive mandatory overtime, and high turnover at the NTC-P could lead to human error due to fatigue or inexperience. Recruitment and retention could be improved if the NTC-P increases its staff, rebuilds the NTC-P analytical functions, and provides a clearer career path for targeting specialists.

DHS has three small-scale programs operating at a limited number of locations that enhance assessment of foreign nationals for those locations: the ICE Visa Security Program, the CBP Immigration Advisory Program, and the USCG BASS. These programs prevent entry into the United States by dangerous and inadmissible foreign nationals, prior to their arrival in the United States, and therefore merit additional funding and expansion.

DHS officers who work overseas must routinely use up to 17 different DHS systems. A single sign-on to some of these systems would improve productivity. A portal on the DHS intranet could streamline access to web-based DHS systems and could assist officers to verify that their queries locate accurate and current information. Web-based training on immigration law, DHS programs, and DHS data systems could also assist overseas officers, who are expected to cover a broader range of immigration-related issues than their domestic counterparts.

Valuable DHS Information-Sharing Initiatives Represent Progress, But Integration Is Advancing Slowly

DHS Components Share Information on Foreign Nationals Despite Challenging Conditions and Fragmented Systems

DHS has a complex mission to track and evaluate foreign nationals. DHS must guard against terrorism; secure borders and control land, sea, and air ports of entry; facilitate legitimate travel; and provide eligible applicants with immigrant and nonimmigrant benefits. DHS databases are a disparate range of systems developed over decades to fulfill these missions. The foreign nationals DHS tracks range from lawful permanent residents to Visa Waiver Program applicants overseas. Data systems were built with different requirements for privacy, records retention, and protection of law enforcement–sensitive information. Different operational missions require varying levels of information: a CBP IAP officer who advises an air carrier against boarding a passenger on the TSDB no fly watch list needs more timely information but less detail than an ICE officer who searches for possible associates of a human smuggler.

Within DHS, funding to improve and integrate data systems comes primarily from the budgets of individual operational components. In addition, operational components that have had limited success with past modernization projects are cautious. For example, after several unsuccessful attempts to migrate all of its records to a new system, the USCIS planned upgrade will transfer limited historical information into its new system under the "Transformation" process. ICE plans to replace its Immigration Enforcement Operational Records System (ENFORCE) databases one at a time rather than to upgrade the whole system at once.

The long-term vision for DHS information sharing on foreign nationals is to provide authorized DHS users with a real-time overview of all information about an individual by aggregating information on each individual from all relevant DHS data systems in what is termed a Person Centric View. In the long term, DHS would also have the analytical software to conduct trend and data analysis on real-time information across systems. However, given the complexity of these goals and limited funding, the headquarters components that will coordinate implementation of this plan told us that it is likely that DHS will continue to operate with a fragmented patchwork of legacy and single-purpose systems for at least three to five more years.

DHS components have cooperated to improve information sharing on foreign nationals. For example, components that plan to upgrade major data systems, such as the USCIS immigration case tracking databases and CBP TECS, have solicited suggestions from users in other components. Several DHS headquarters offices, including the Information Sharing and Collaboration Branch, the Screening Coordination Office, and the Counterterrorism Section in the Office of Operations Coordination and Planning, have coordinated with operational components to identify best practices and data gaps.

DHS has also recently given more authority to the Office of Intelligence and Analysis, the Office of the Chief Information Officer, and the Screening Coordination Office to begin integration of data systems and prioritize expenditures. The DHS Information Sharing Governance Board and the government-wide Interagency Policy Council on Information Sharing and Access are among the institutional forums where better coordination of information sharing will be developed. Most of these initiatives are in the early stages, as the functions of hundreds of DHS data systems must be mapped. There is general agreement among these DHS stakeholders on a methodology to integrate information, which will assist planning. Integration will focus on the development or adaptation of software that can search and analyze existing data systems in real time. With the exception of USCIS Transformation, there will be few attempts to consolidate information from existing data systems.

Close cooperation among operational components that first encounter foreign nationals overseas has helped overcome some of the challenges presented by DHS data systems. Many of the officers we interviewed attributed successful working relations to the personalities and professionalism of their colleagues, rather than the effect of formal policies that require information sharing. The overseas officers we interviewed cooperated well when their missions overlapped. In addition, overseas officers obtained informal assistance from the NTC-P and DHS officers familiar with immigration law and the more complex databases. We also observed strong working relationships among the NTC-P, Regional Carrier Liaison Groups, and IAP officers, who often must work together to resolve potential no fly and do not board matches in 30 minutes or less. For interdictions at sea, the USCG, US-VISIT, and CBP have developed an effective program to share information on migrants who make repeated attempts to enter the United States without permission.

Centralization of IDENT Biometrics Screening Is Essential to Information Sharing

We consider that the most important building block for successful information sharing within DHS is the US-VISIT biometric fingerprint IDENT, because fingerprints establish a unique identity for each foreign national even when biographic information and travel documents change. The ability to establish and verify identity through fingerprint enrollment is the most accurate means to track known and suspected terrorists, criminals, and migrants with false or multiple identities, as well as to facilitate legitimate travel and benefits administration. DHS has designated IDENT as its primary repository of biometric information in the enforcement of civil and criminal laws, and national security and intelligence activities.

Most foreign nationals who: (1) apply for a visa or refugee status overseas; (2) arrive at an international airport in the United States; (3) apply for an immigration benefit; or (4) are detained, are enrolled in IDENT. The USCG enrolls some interdicted migrants, and CBP enrolls some land border crossers. In 2009, IDENT largely completed its transition from a two-fingerprint enrollment system to a full ten-fingerprint enrollment, which provides greater interoperability with FBI biometric systems. Ten-fingerprint compatibility allows DHS to query fingerprints against prior enrollments under other names or identities in the United States, or in countries that share fingerprint information from criminal records. IDENT is also used to compare fingerprints lifted from terrorist safe houses or battlefields. The governments of the United States, Australia, Canada, New Zealand, and the United Kingdom now compare fingerprints via their biometric databases to identify fugitives and individuals who have falsified identities. IDENT has fundamentally transformed information sharing.

Congressional mandates to expand US-VISIT biometric enrollment —most notably exit controls at borders—will require significant increases in funding and infrastructure.[23] However, realistic shorter-term projects could be accomplished with existing technology and more limited funding, but they have been delayed because US-VISIT has not been able to secure signatures on agreements or because logistical challenges have not been resolved. IDENT is the primary repository for biometrics for foreign nationals throughout the federal government. However, some DHS biometrics are not automatically integrated into IDENT, such as fingerprints obtained through TSA's Transportation Worker Identification Credential (TWIC) program, which is required for unescorted access to secure areas of designated maritime ports.[24] Some individuals who are issued TWIC credentials, which can include truck drivers and dock workers as well as USCG documented merchant mariners, are foreign nationals or naturalized citizens. Biometric information should be checked automatically against other biometric-based information available in IDENT from DHS and the State Department.

IDENT checks known or suspected terrorist biometrics against FBI biometric systems, but some biometric and biographic records in the National Counterterrorism Center are not yet automatically

[23] P.L. 108-458

[24] P.L. 107-295

checked against US-VISIT. The Department of Defense is addressing logistical impediments to its ability to share biometrics in its Automated Biometric Identification System, to compare Department of Defense fingerprints automatically, rather than on a case-by-case basis, and is looking to build directly into IDENT. Each of these initiatives would eliminate or reduce potential gaps in the information currently available to the federal government on potential terrorists, criminals, and unauthorized foreign nationals.

Recommendations

We recommend that the Office of Policy, and U.S. Visitor and Immigrant Status Indicator Technology:

Recommendation #1: Coordinate and work with the DHS people screening programs which collect biometrics to use US-VISIT IDENT for their biometric storage and matching requirements.

Recommendation #2: Work with other federal agencies to share biometrics of foreign nationals collected by those agencies with DHS US-VISIT IDENT.

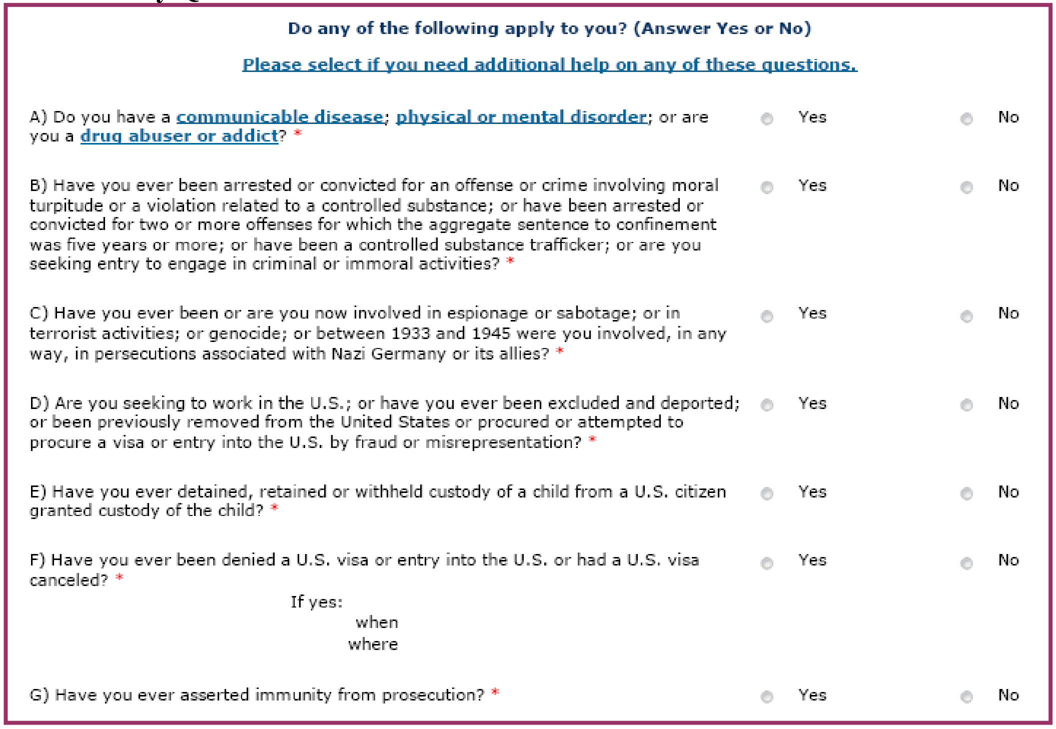
Upgrades to ESTA Website Would Reduce Deficits

In addition to relatively modest changes to IDENT, information sharing could be substantially improved if DHS invested in improvements to the ESTA website to reduce inefficiencies created by inaccurate data submissions. CBP officers reported numerous submission errors on the ESTA applications because applicants misunderstood the eligibility questions. As shown in the ESTA website extract (Figure 4), the application includes a series of questions about admissibility to the United States, but a full definition of the grounds for inadmissibility requires applicants to click on a hyperlink. An official from the CBP ESTA program noted that travelers routinely answer certain questions incorrectly because users do not read these definitions. Most notably, Question A, on communicable diseases and Question G, on immunity from prosecution, are inappropriately marked “Yes.” Applicants may mark that they have communicable diseases, but they are not diseases the Department of Health and Human Services would consider to be of public health significance and are therefore grounds for inadmissibility.[25] Applicants may mark that they have a physical disorder because they are in a wheelchair,

[25] 8 U.S.C. 1182 (a) (1) (A) (iii) (I).

while the regulations bar travel only by individuals who present a threat to property, safety, or welfare.[26] Applicants who mark that they have asserted immunity from prosecution may be in a civil dispute with a neighbor but have not committed a serious crime in the United States.[27]

Figure 4: Visa Waiver Program Country Website Interface – Admissibility Questions



Do any of the following apply to you? (Answer Yes or No)

Please select if you need additional help on any of these questions.

A) Do you have a communicable disease; physical or mental disorder; or are you a drug abuser or addict? *	○ Yes	○ No
B) Have you ever been arrested or convicted for an offense or crime involving moral turpitude or a violation related to a controlled substance; or have been arrested or convicted for two or more offenses for which the aggregate sentence to confinement was five years or more; or have been a controlled substance trafficker; or are you seeking entry to engage in criminal or immoral activities? *	○ Yes	○ No
C) Have you ever been or are you now involved in espionage or sabotage; or in terrorist activities; or genocide; or between 1933 and 1945 were you involved, in any way, in persecutions associated with Nazi Germany or its allies? *	○ Yes	○ No
D) Are you seeking to work in the U.S.; or have you ever been excluded and deported; or been previously removed from the United States or procured or attempted to procure a visa or entry into the U.S. by fraud or misrepresentation? *	○ Yes	○ No
E) Have you ever detained, retained or withheld custody of a child from a U.S. citizen granted custody of the child? *	○ Yes	○ No
F) Have you ever been denied a U.S. visa or entry into the U.S. or had a U.S. visa canceled? * If yes: when where	○ Yes	○ No
G) Have you ever asserted immunity from prosecution? *	○ Yes	○ No

Source: ESTA website user interface (www.cbp.gov)

When ESTA applicants mark "Yes" for a question that is known to be widely misunderstood, the NTC-P ESTA division, the ESTA program management office at CBP headquarters, IAP officers, or the Regional Carrier Liaison Group may attempt to reconcile the issue through research of immigration and criminal records. They may also discuss the concerns with the applicant or airline, which may be able to provide additional biographic or documentary information to resolve them. If there is no additional derogatory information, a CBP officer may manually approve the ESTA application. IAP officers report that when they have cleared higher priority cases, they spend considerable time on ESTA cases. They try to resolve cases that appear to be based on a misunderstanding of the application, but the volume is too high to resolve all cases,

[26] 8 U.S.C. 1182 (a) (1) (A) (iii).
[27] 8 U.S.C. 1182 (a) (2) (E).

and some applicants are not permitted to travel on that day and must instead seek an appointment with the State Department to apply for a visa. ESTA program managers have tried to address the issue through information provided in hyperlinks, and through asking applicants to verify their "Yes" response to Question A, but they told us that major improvements to the ESTA website will not be introduced until ESTA transitions to a fee-based program and collects sufficient funds to make database changes.[28]

In addition, the ESTA data entry interface allows applicants to enter incorrect passport numbers, for example substituting a letter "O" for a zero, so the ESTA travel authorization approval that the applicant brings to the airport may not match the machine-readable passport. ESTA program managers told us that through experience and communication with visa waiver governments they have identified passport numbering conventions that could be used to catch some incorrect data entry by applicants. Immigration Advisory Program officers reported that it can be difficult for air carriers to locate an approved ESTA within their system, and to decide whether or not to rely on the printed approval. In these and other instances where there appears to be an innocent error, such as a misspelling or a transposition of a date of birth, CBP may direct travelers to apply for a new ESTA approval at the airport.

When CBP, travelers, and airlines are aware that there is a relatively high incidence of innocent errors in ESTA applications, the benefit of doubt that is extended to travelers can leave the system more open to potential abuse. The ESTA program will transition to a fee-based application process, and will therefore need to develop an application that can be amended rather than discarded and replaced when there are errors. With a new design, the ESTA program has an opportunity to limit some common data entry and matching challenges. As discussed in more detail later in the report, the ESTA program also generates cases of applicants who may have correctly marked "Yes" on an application, but whose applications CBP can resolve if it has the staff resources. For example, CBP may determine that it is not necessary to deny the ESTA application of persons who self-report that they were denied a student visa a decade ago, but against whom there is no other derogatory information. Improvements to the website would allow CBP to devote more resources to these cases and reduce the need to refer such applicants to a consulate for resolution.

[28] The ESTA program implemented a fee of $14 in September 2010, after we completed field work.

Recommendations

We recommend that U.S. Customs and Border Protection:

Recommendation #3: Amend the Electronic System for Travel Authorization website to address the most common areas of confusion that participating travelers from Visa Waiver Program countries have with regulatory language when they complete Electronic System for Travel Authorization applications.

Recommendation #4: Amend the Electronic System for Travel Authorization website to limit potential for incorrect applicant information and inappropriate denials.

Shared Mission Communities Can Assist Long-Term DHS Data Systems Improvements

CBP can improve ESTA. Improvements to IDENT require only cooperation between US-VISIT, TSA, and headquarters staff responsible for negotiating interagency agreements. However, more complex upgrades to and coordination among data systems owned by CBP, ICE, TSA, and USCIS, and used throughout federal, state, local, and tribal governments, would best be planned in the context of the Shared Mission Communities. Shared Mission Communities provide an official DHS forum for components to integrate their activities and are effective because they can raise issues that require financial commitments or a binding decision to the Information Sharing Governance Board. The Under Secretary for Intelligence and Analysis, who chairs the Information Sharing Governance Board, was recently designated the lead on initiatives to prioritize financial commitments and efforts to consolidate information in DHS data systems.

The work of the two current Shared Mission Communities—Law Enforcement and Intelligence—has improved information sharing on foreign nationals. A third Shared Mission Community on Border Security would provide immigration and border management components a framework to improve information sharing and identify gaps and redundancies in the information available in DHS data systems.

In its 2009 Annual Report, the Information Sharing Governance Board recognized the accomplishments of the Law Enforcement and Intelligence Shared Mission Communities. The board recommended establishment of others, including Infrastructure Protection, Incident Management, Border Security, and Transportation Security. The Shared Mission Communities can be used to "identify, promote, and champion resource alignment" to support shared missions, and as a "forum for discussion of mission-specific issues to ensure that the mission voice is represented in departmental information sharing decisions."[29]

Shared Mission Communities can include many of the same components, and even many of the same offices within components. For example, CBP, ICE, TSA, the USCG, and USCIS could be integral to several Shared Mission Communities. The value of a Border Security Shared Mission Community is that it can focus on specific issues and strategies, including targeting, screening, biometric enrollment, and possible expansion of exit controls. A Border Security Shared Mission Community could also be a forum for obtaining resources to extend the use of some of the most sophisticated DHS targeting and analysis software, such as the CBP Automated Targeting System–Passenger (ATS-P), and geospatial software developed by the CBP Border Patrol.

Recommendation

We recommend that the Office of Intelligence and Analysis:

Recommendation #5: Submit a proposal to the Information Sharing Governance Board to consider establishing a Border Security Shared Mission Community.

Management Comments and OIG Analysis

Management Comments: The Office of Policy, and U.S. Visitor and Immigrant Status Indicator Technology, concurred with Recommendation #1 [Coordinate and work with the DHS people screening programs which collect biometrics to use US-VISIT IDENT for their biometric storage and matching requirements]. The Office of Policy stated that on May 25, 2007, a memorandum was issued to the Chief Information Officers (CIOs) of ICE, CBP, USCIS, TSA, and US-VISIT, directing that all DHS programs that require the collection and use of fingerprints to vet individuals, shall use the target biometric service as defined by the Homeland Security Enterprise Architecture –IDENT. The Office of Policy

[29] Information Sharing Governance Board Annual Report 2009, May 8, 2009, p. 10.

advised that IDENT for biometric storage and matching is being used by USCIS, CBP, and ICE. Also, the Office of Policy said that TSA is transitioning to US-VISIT's IDENT for similar purposes.

OIG Analysis: This recommendation is *resolved and open.* The Office of Policy's actions planned are responsive to the recommendation. The Office of Policy shows a level of commitment in implementing guidelines requiring DHS components that collect biometric information to use IDENT for their storage and matching requirements. Please provide detailed information, such as reports, memorandums or technical plans, as well as timelines, on TSA's plan for transitioning to using US-VISIT IDENT for biometric storage and matching.

Management Comments: The Office of Policy, and U.S. Visitor and Immigrant Status Indicator Technology, concurred with Recommendation #2 [Work with other federal agencies to share biometrics of foreign nationals collected by those agencies with DHS US-VISIT IDENT]. The Office of Policy stated that DHS has ongoing efforts with other federal agencies, especially those within the Intelligence and Defense communities, to check and store the fingerprint biometrics they capture within IDENT.

OIG Analysis: This recommendation is *resolved and open.* Please provide copies of meeting minutes or other records to document that the Office of Policy has met and continues to meet with other federal agencies to effect automated checking and storage of biometric information on foreign nationals within IDENT. Please include information on any barriers to implementation, such as resource needs or technological challenges.

Management Comments: CBP concurred with Recommendation #3 [Amend the ESTA website to address the most common areas of confusion that participating travelers from Visa Waiver Program countries have with regulatory language when they complete ESTA applications]. CBP said that the changes recommended in the report were completed in the ESTA website on September 8, 2010, after our fieldwork was completed, in a major upgrade to the website. In addition to adding fee provisions, CBP said that it made additional changes to help Visa Waiver Program (VWP) applications, for example: 1) Those who mistakenly answer yes to Question A or G can now reapply and receive an approval without CBP intervention; and 2) the programming rules for some country passports have been refined to help prevent applicants from being turned around at the airport or denied entry upon arrival in the United States. A more complete list of examples is provided in the management comments in Appendix B.

OIG Analysis: This recommendation is *resolved and open.* The changes described appear to meet our requirements. We request an update with additional details on two of the described changes. For the reapplication with Questions A and G, please describe how CBP determines that the original answer was simply a mistake, and whether the fee is waived for a reapplication. For the upgraded programming rules for some country passports, please provide a few specific examples so that we understand the methodology. These responses can be provided in an informal email. As soon as we receive this information, we will consider this recommendation resolved and closed. We commend CBP for the rapid response to these areas of confusion.

Management Comments: CBP concurred with Recommendation #4 [Amend the ESTA website to limit potential for incorrect applicant information and inappropriate denials]. CBP said that it continues to make significant changes to the ESTA website as necessary. CBP said that it carefully monitors the ESTA applications to ensure that applicants are not trying to work around the system. With the implementation of the fee CBP said that it anticipates fewer applicants gaming the system, as they will be required to pay for each new application. CBP noted that ESTA is a system that is generated by the applicants in the general public. CBP said as long as the general public enters information, there will be entry errors, most often with passport numbers. Until the public becomes aware of these data elements, there will be mistakes. CBP said that it continues to monitor customer feedback and make amendments to the website as needed.

OIG Analysis: This recommendation is *resolved and open.* Please provide an update on some of the amendments that have been made to the website from CBP monitoring of the applications, or in response to customer comments. We agree that some entry errors will remain inevitable with the public entering information. We are not persuaded that the small incremental costs of multiple ESTA applications will deter persons ineligible for the Visa Waiver Program from attempting to avoid applying for a visa.

Management Comments: The Office of Intelligence and Analysis, and CBP, did not concur with Recommendation #5 [Submit a proposal to the Information Sharing Governance Board to consider establishing a Border Security Shared Mission Community]. The Office of Intelligence and Analysis stated that a Border Security Shared Mission Community would duplicate other organizations' activities underway and would not measurably improve information sharing among DHS components with relevant equities in border security beyond that which is already occurring. The Office of Intelligence and Analysis stated these organizations include the Border Intelligence Fusion Section, composed of participants from DHS and other interagency partners; and the State of the Border, which focuses on Southwest Border law enforcement activities with plans to expand the area of focus to Northern Border and coastal environments.

OIG Analysis: This recommendation is *unresolved and open.* We believe the actions planned by the Office of Intelligence and Analysis are not responsive to the recommendation. Although the Office of Intelligence and Analysis consulted with CBP, these views may not represent the other entities responsible for border security. The actions as described do not provide sufficient details regarding how all components integrally involved with border security information sharing, such as ICE and USCIS, are represented in the Border Intelligence Fusion Section and the State of the Border organizations. As described, these organizations appear to focus on the details of current operations, and are limited to land and coastal borders. They do not appear to have a mandate to address longer-term coordination of data system upgrades necessary to enhance border security. It is possible that one of these organizations could assume the responsibilities for a unified information sharing role as the Border Security Shared Mission Community.

This recommendation will remain unresolved and open until the Office of Intelligence and Analysis submits a proposal to the Information Sharing Governance Board to consider establishing a Border Security Shared Mission Community. The decision would include all DHS components with a border security nexus, to determine if there is consensus on whether to establish a Border Security Shared Mission Community. The Border Security Shared Mission Community would include components such as USCIS with relevant data systems. If the Information Sharing Governance Board decides not to establish this Shared Mission Community at that time, we will consider the recommendation resolved and closed.

NTC-P Can Improve Effectiveness by Improving Working Conditions

NTC-P Counterterrorism Screening Relies on Fragmented Data Systems and Incomplete Information

The NTC-P is the operational core of DHS antiterrorism passenger screening efforts for air and land borders. The NTC-P partners with the USCG when screening passengers and crews for maritime border threats. The NTC-P provides significant travel screening assets and resources to DHS officers and federal partners. Its responsibilities and workload increase with every new potential threat. In response to the December 2009 bombing attempt, the NTC-P must now review possible hits against an expanded TSDB watch list and additional Department of State visa revocations. In addition, the NTC-P increased its pre-departure screening of international flights. Although the primary responsibility of the NTC-P is to screen travelers' flights and vessels, it also receives and responds to hundreds of calls daily from law enforcement and intelligence officers for information housed in DHS data systems. Adequate resources, which include staff and data systems, are essential if the NTC-P is to respond quickly to information on potential threats.

Many federal data systems contain relevant data on foreign nationals. These systems are not well integrated and were originally designed for other purposes, which makes screening passengers against potentially derogatory information a labor-intensive process. NTC-P targeting specialists use as many as four computer monitors with different databases open concurrently to resolve possible matches identified through the targeting software, ATS-P. They must continually transfer information from one system into another. When possible matches cannot be resolved, targeting specialists must log into numerous additional databases to determine whether a traveler is an individual in a watch list record, or whether potentially derogatory information is accurate.

To determine the accuracy of any given possible match, it might be necessary to query TECS, APIS, ESTA, Student and Exchange Visitor Information System (SEVIS), ENFORCE, USCIS systems and verify information contained in Central Index System (CIS), Computer-Linked Application Information Management System 3 (CLAIMS3), Image Storage and Retrieval System (ISRS), and US-VISIT IDENT and Arrival and Departure Information System (ADIS). It may also be necessary to check databases owned by other federal agencies, such as the Department of State Consular Consolidated Database, and commercial databases, such as those used for credit reporting. Figure 5 illustrates some of the difficulties NTC-P targeting specialists must overcome when they use the systems to evaluate possible derogatory information.

Figure 5: Difficulties in Navigating DHS Data Systems

Sample System Check Processes

To search systems requires understanding how the database is structured:

- ➢ IDENT is organized by fingerprint identification number
- ➢ CIS is organized by case number or alien number
- ➢ ENFORCE is organized by event

In some cases it is necessary to check one DHS or State Department database to obtain a record locator to query another database:

- ➢ Using SEVIS may require checking the State Department visa issuance database first
- ➢ Most checks of IDENT require obtaining a fingerprint identification number from another DHS database such as CLAIMS3

DHS databases match biographic information with different methods and levels of accuracy:

- ➢ Systems like ATS-P can identify near matches (John Smith, Jonathan Smith, and Jon Smythe)
- ➢ Systems like SEVIS are searchable only within a visa type

Databases have known idiosyncrasies that require further checks for false positive and false negative matches:

- ➢ ESTA matches ethnic Irish names starting with the letter "O'" (O'Reilly may match against O'Keefe)
- ➢ Users of the older USCIS systems report that sometimes an exact name spelling will not locate a record

When a data system is programmed to transfer information to another system, experienced users check the records in both systems, because sometimes only part of the original data has been transferred:

- ➢ Information in ATS-P needs to be checked against TECS
- ➢ CIS needs to be checked against Image Storage and Retrieval System (ISRS)

Targeting specialists and officers using DHS systems for research need to understand the methodology used to include data in specific databases:

- ➢ APIS does not always accurately reflect who has actually traveled, and must be checked against Arrival and Departure Information System (ADIS)
- ➢ TECS includes individuals against whom potentially derogatory information was resolved

Source: DHS database demonstrations, training materials, interviews

[redacted]

Under current regulations, DHS has access to passenger ticketing information, Passenger Name Record (PNR), collected by airlines up to 72 hours in advance of departure (see figure 3 above). CBP receives PNR data periodically and conducts analysis as necessary until [redacted] before departure. PNR data are unverified and may be incomplete. [redacted]

With APIS, airlines may provide a manifest with full information on all passengers as late as 30 minutes before a flight departs, or if certified to use APIS Quick Query, may transmit information on individual passengers as late as when the aircraft door is closed for departure. [redacted] The consequences to date have been passenger offloads with flight delays, flight diversions, and passengers denied admission on arrival and placed in costly removal proceedings.

As of November 23, 2010, Secure Flight completed deployment for all U.S. aircraft operators and foreign air carriers with commercial flights into, out of, and within the United States, and will establish a timeline to expand to flights in transit over the continental United States. Secure Flight watch list matching may enhance the security of commercial air travel by improving the watch list matching process. Securing the distribution of watch list data and expediting law enforcement identification should reduce the number of misidentified passengers. Although, Secure Flight provides a discrete set of information necessary for effective screening sooner, the information is self-reported. APIS information is generally the first verified data DHS receives. The NTC-P may require country of citizenship and travel document information from APIS to resolve whether the passenger is a possible match to the TSDB watch list.

[redacted]

In 2006, when DHS evaluated changes to regulations on passenger manifests, it considered whether to require airlines to provide APIS information earlier. However, the study estimated that it could cost airlines $1.9 billion over a decade to provide more timely information. Technology upgrades would be necessary to transmit PNR data more frequently to CBP data systems. Response times could be improved somewhat with increased staff at the NTC-P, Regional Carrier Liaison Groups, and Immigration Advisory Program, and more carrier liaison training and outreach. The NTC-P managers and Regional Carrier Liaison Group officers we interviewed said that they did not have sufficient staff and travel budgets to maintain optimal relationships with foreign carriers.

Recommendation

We recommend that U.S. Customs and Border Protection:

Recommendation #6: Assess options for obtaining Advance Passenger Information System data from carriers earlier, and Passenger Name Record data from reservation systems more frequently, in a manner that is cost-effective.

Additional Liaisons Will Contribute to NTC-P Effectiveness

DHS components have provided the NTC-P with the liaison personnel it has requested. Additional support from other federal agencies would enhance the ability of the NTC-P to screen matches quickly and accurately. Liaisons provide the NTC-P with immediate access to restricted databases managed by their host organizations. Liaisons also interpret complex case information in those databases, and can ensure a rapid threat response from their agency. Non-DHS personnel detailed to the NTC-P can also conduct research for their own investigations with information from NTC-P experts or DHS databases. The NTC-P currently has DHS liaisons from several components: ICE, TSA Office of Intelligence, TSA Federal Air Marshal Service, the USCIS Fraud Detection and National Security Directorate, and the USCG.

However, there are relatively few liaisons from other federal government agencies. For example, the FBI sought the May 2010 Times Square bombing suspect when he was identified through the NTC-P review of APIS passenger manifests. This illustrates the need for close cooperation between the NTC-P and FBI. However, the FBI does not currently have a NTC-P liaison. NTC-P managers told us that there had been an FBI presence in the past and they are currently negotiating to re-establish a liaison. The Centers for Disease Control and Prevention also does not have staff at the NTC-P. Centers for Disease Control and Prevention's public health do not board list, which currently includes fewer than 100 names, provides information on individuals believed to pose a potential health threat. However, any potential health threat that includes individuals who were not yet on the list can require the NTC-P and Centers for Disease Control and Prevention to locate every passenger on an airplane or vessel. NTC-P managers said that a liaison could conduct many of the database queries that targeting specialists currently conduct. The Department of State provides one full-time liaison, but NTC-P managers said that on evenings and weekends when their liaison is no longer on site it can be difficult to obtain information to respond to visa revocation issues.

Other federal members of the intelligence community do not have a liaison at the NTC-P, so the NTC-P relies on CBP members of the TSC and Joint Terrorism Task Forces to conduct liaison on their behalf. The time-sensitive nature of the NTC-P mission merits onsite support.

Recommendation

We recommend that U.S. Customs and Border Protection:

Recommendation #7: Request liaisons from the Department of Justice Federal Bureau of Investigation and the Department of Health and Human Services Centers for Disease Control and Prevention, key partners for no fly and do not board cases, to participate at the National Targeting Center – Passenger.

NTC-P Staffing Challenges Persist

Policy changes in response to the recent bombing attempts increased the NTC-P workload. To assess whether the NTC-P had sufficient staff, we interviewed senior NTC-P managers, Watch Commanders, and targeting specialists. We also interviewed former NTC-P senior managers, former detailed and permanent staff, and officials from the Regional Carrier Liaison Groups and overseas operations who work closely with the NTC-P. We reviewed assessments that the NTC-P conducted on staff resources, recruitment, and retention, surveys they conducted with current staff, and exit interviews. Additionally, two inspectors observed operations at the NTC-P for a week.

We concluded that the NTC-P does not have sufficient staff to manage the workload. From March 2009 to March 2010, there were 54,041 FBI TSDB watch list possible matches, and the volume will rise with expansion of the TSDB no fly and selectee watch lists. In calendar year 2009, the NTC-P resolved 47,103 ESTA cases. The number of these cases will grow considerably in 2010 because it is now mandatory for participating travelers from Visa Waiver Program countries to apply for an approved ESTA travel authorization in advance of travel to the United States. The NTC-P responds to hundreds of calls daily from federal law enforcement, intelligence, and immigration officers. It also has desks that: (1) cover visa revocations and do not board cases; (2) support Immigration Advisory Program officers; (3) screen inbound and outbound flights; and (4) support screening coordination with foreign governments, which include Canada and the United Kingdom.

NTC-P managers estimated that they would need about 230 additional staff to effectively manage the caseload. This staffing level would enable additional targeting specialists to work on each of the NTC-P desks and still cover training and leave requirements. Before the December 2009 bombing attempt, the NTC-P announced 25 vacancies, but hiring did not occur due to budget restrictions. Since then, the NTC-P obtained some temporary duty (TDY) employees from CBP ports of entry and from the CBP Border Patrol to supplement existing staff. The NTC-P has recently advertised for an additional 20 temporary positions to be spread throughout the multiple shifts. The NTC-P would need to increase the number of positions further to have sufficient staff for each shift.

The NTC-P currently addresses its staffing shortages with heavy use of overtime (200%), administratively uncontrollable overtime, and TDY staff recruited from the field offices. In some cases, targeting specialists work up to four additional hours after their original shift without advance notice. Every day we observed a Watch Commander call staff at home throughout the morning to try to find staff to work additional overtime hours to cover high-priority desks. Reliance on mandatory overtime to address staffing shortfalls for an extended period has become ineffective, as staff turnover and sick leave usage is prevalent.

The NTC-P has also moved staff from lower vetting priorities to cover possible no fly and do not board matches. The cases that now receive lower priority include aggravated felons who attempt to enter the United States, visa revocation cases, and ESTA denials. If the NTC-P misses a match to derogatory information and therefore does not prevent the traveler from boarding, these inadmissible aliens arrive at domestic ports of entry. Inadmissible aliens who arrive at ports of entry add to the workload of DHS officers, immigration judges, and government attorneys. All inadmissible aliens must be questioned and detained for removal, and many must be placed in removal proceedings before an immigration judge, with an ICE attorney to represent the government in the proceedings. In addition, the NTC-P is mandated to notify federal, state, tribal, and local law enforcement when an individual under a warrant attempts to flee the country, but staff conduct these searches only when time permits.

Additional staff would allow the NTC-P to resume these essential law enforcement functions, respond adequately to crisis situations, provide screening for national security special events, and assist staff who must vet multiple hits on short notice.

Staff constraints have also led the NTC-P to curtail its information collection and data analysis. CBP officers at ports of entry, and Immigration Advisory Program officers at overseas airports, collect and report information on travelers who have been questioned due to an unresolved TECS record. The information can include names, telephone numbers, addresses, and second passports or identity documents in other names. When checked, these leads can provide a key link between travelers who were interviewed and known or suspected terrorists or criminals, or organized immigration fraud. We observed a targeting specialist on the Advance Targeting Team (ATT) conducting link analysis on potential associates of a financial fraud ring; the officer said that the team can work these cases only when their time was not devoted to higher priority screening.

Time for other than higher priority screening is increasingly rare for NTC-P staff. Other CBP units that conducted link and trend analysis on passengers, such as the Regional Carrier Liaison Group, told us they no longer are able to do much analysis given their expanding workload. Officials we interviewed throughout DHS singled out the skills of the more experienced targeting specialists at the NTC-P, and the screening software used by CBP—ATS-P—as the most sophisticated analysis resources currently available in DHS. NTC-P managers said they could rebuild the NTC-P ATT link and data analysis capabilities with a staff of 230 officers. We consider this a reasonable investment in the ability of DHS to "connect the dots" in terrorism and criminal cases.

Recommendations

We recommend that U.S. Customs and Border Protection:

Recommendation #8: Increase full-time or temporary duty staff to a minimum of 230 Customs and Border Protection officers at the National Targeting Center – Passenger.

Recommendation #9: Dedicate full-time or temporary duty staff at the National Targeting Center – Passenger to expand the Advance Targeting Team so that the team can conduct data analysis and follow up on leads other Customs and Border Protection Officers develop.

NTC-P Staff Recruitment and Retention Needs Improvement

Increasing the number of positions at the NTC-P will alleviate staffing shortages only if the NTC-P also addresses chronic difficulties with recruiting and retaining staff. Current and former NTC-P staff and managers commented that additional NTC-P responsibilities since the December 2009 bombing attempt have added stress to an already strained workforce. Managers informed us that in 2008, the NTC-P conducted a study of its recruitment and retention problems, but did not implement recommendations due to insufficient staff to cover proposed changes. The NTC-P has discontinued programs and initiatives which could improve work-life balance and staff retention if reinstated. For example, in surveys, exit interviews, and staff meetings, targeting specialists identified the availability of an alternate work schedule, which exchanges a longer workday for an extra day off each week or each pay period, as a strong retention incentive.

Current and former staff and senior managers at the NTC-P told us that recruitment and retention at the NTC-P are more difficult because targeting specialists do not have a clear career path for advancement either at the NTC-P or elsewhere in CBP. Studies that the NTC-P conducted in 2008 on staff retention confirmed this assessment, as targeting specialists cited the need for a promotional path as a factor in choosing to leave. The career path of targeting specialists stops at a non-supervisory position. It can be difficult for specialists to demonstrate relevant experience to compete for supervisory positions. NTC-P managers currently offer temporary supervisory assignments to provide such experience, but staff shortages limit these assignments.

The level of responsibility, the need to operate under stressful conditions, and time constraints at the NTC-P are comparable to the work officers at the same grade level performed at CBP headquarters. However, NTC-P managers said that most field managers do not recognize a tour of duty at the NTC-P as comparable to a headquarters tour of duty. Current NTC-P managers said that additional training for more experienced staff on the databases and underlying immigration laws would benefit the NTC-P and enhance the skills of targeting specialists for promotion to other CBP positions. Current and former NTC-P managers said that if the NTC-P created more analytical positions with the ATT, it would provide an incentive for the best targeting specialists to remain, either with the opportunity for a temporary assignment to conduct data analysis or as a more permanent career path.

Recommendations

We recommend that U.S. Customs and Border Protection:

Recommendation #10: Develop and implement work/life balance programs that will promote staff retention at the National Targeting Center – Passenger.

Recommendation #11: Develop a program for career advancement within the National Targeting Center – Passenger that includes necessary cross-training opportunities and a career ladder to better enable qualified analysts and targeting specialists to compete for advancement to senior analyst or supervisory positions.

Management Comments and OIG Analysis

Management Comments: CBP concurred with Recommendation #6 [Assess options for obtaining APIS data from carriers earlier, and PNR data from reservation systems more frequently, in a manner that is cost-effective]. CBP said that it will conduct an assessment to identify options for obtaining APIS data earlier in the travel process and provide anticipated benefits and impacts with each to determine if the benefits gained from such a change outweigh the impacts. CBP noted that it had previously proposed requiring APIS data 60 minutes prior to departure, but numerous comments from the industry indicated that this option would place an unreasonable burden on carrier operations. CBP said that it would assess the current times for PNR data provisions to identify if modifications in these timeframes would provide PNR information more timely for increased targeting efficiency. CBP stated that the air carrier industry has also previously indicated they would like to reduce the number of times they provide PNR data due to costs, which presents challenges for increasing the frequency of accessing PNR data.

OIG Analysis: This recommendation is *resolved and open.* Please provide an update on CBP's assessment of these options, including information on the likely costs of both options. We recognize that CBP may conclude from its cost-benefit analysis that such improvements are not financially feasible.

Management Comments: CBP concurred with Recommendation #7 [Request liaisons from the Department of Justice Federal Bureau of Investigation and the Department of Health and Human Services Centers for Disease Control and Prevention, key partners for no fly and do not board cases, to participate at the NTC-P]. CBP stated that the NTC-P and Centers for Disease Control and Prevention are in discussions with Centers for Disease Control and Prevention liaison to establish a presence at the NTC-P. CBP stated that communication/IT infrastructure for FBI liaison is currently being installed.

OIG Analysis: This recommendation is *resolved and open.* Please provide an update on the efforts CBP has taken to secure liaisons from these agencies. We recognize that CBP does not have the authority to require other federal agencies to provide liaisons, and will close this recommendation based on CBP's efforts rather than on a specific outcome.

Management Comments: CBP concurred in part with Recommendation #8 [Increase full-time or TDY staff to a minimum of 230 Customs and Border Protection officers at the NTC-P]. CBP stated that the 230 CBP officers mentioned in the recommendation includes managerial, supervisory, administrative, and support staff, and is an estimate subject to change based on fluctuating targeting dynamics. CBP noted that the NTC-P is also in the process of attempting to get additional permanent officer positions and is trying to reduce the number of TDY officers at the NTC-P. CBP said that the NTC-P has identified the need for 55-75 new permanent officer positions and new, permanent managerial, support and administrative positions to support the additional staff. CBP said that the 55-75 new CBP officer positions are required to adequately staff new or enhanced targeting programs including, Pre-Departure screening, ATT initiatives, Outbound targeting, Visa re-vetting, and expanded Immigration Advisory Program operations. CBP said that the officers would be spread across three shifts, to cover a 24-hour period. CBP said that the allocation of officers to specific shifts and targeting programs is continually evaluated and it is not possible to provide a definitive or static number of officers required per shift due to the fluid nature of the workflow and ever-changing threat streams. CBP said that the due date is dependent upon the availability of personnel to fill the NTC-P vacancies, as well as the availability of funding to hire and move selected officers. CBP noted that in addition to other variables, staff attrition makes it very difficult to maintain a static number of personnel.

OIG Analysis: Based on the specific information CBP provided, we consider this recommendation *resolved and open.* We request that CBP provide the following information: 1) any unanticipated funding or staffing constraints, such as a hiring freeze, that affected staffing; 2) the dates of any announcements for additional permanent staff; 3) the number of permanent staff in CBP officer positions; 4) the number of TDY staff; and 5) statistics or a management report on the workload at the NTC-P. We recognize that the NTC-P must remain flexible in its staffing: for example, improvements to the ESTA website may reduce the ESTA caseload. We also recognize that CBP cannot control all of the factors that affect staffing levels, such as funding and attrition. DHS directives pertaining to resolution by components of OIG recommendations require CBP to update this information every 90 days. If it can be demonstrated that the NTC-P is making good progress towards the goal of 230 staff, or that there are factors outside the control of CBP that prevent adequate staffing levels, we will close the recommendation.

Management Comments: CBP concurred with Recommendation #9 [Dedicate full-time or TDY staff at the NTC-P to expand the ATT so that the team can conduct data analysis and follow up on leads other Customs and Border Protection Officers develop]. CBP said that permanent staffing solutions for the ATT are included in the request for 55-75 new CBP officer positions noted above. CBP noted that the due date is dependent upon the availability of personnel to fill NTC-P vacancies, as well as the availability of funding to actually hire and move selected officers. CBP said that in addition to other variables, staff attrition makes it difficult to maintain a static number of personnel on any given targeting program, such as the ATT, so it is unlikely that a definitive "due date" is attainable or realistic.

OIG Analysis: This recommendation is *resolved and open.* We request that CBP provide evidence of the number of CBP officers working for the ATT. Evidence might include an organizational chart with the names of assigned officers, a staffing roster, or a list compiled specifically for us. We recognize that the NTC-P must remain flexible in its staffing, and that CBP cannot control all of the factors that affect staffing levels. When the NTC-P is making good progress towards increasing the staffing of the ATT, we will close the recommendation.

Management Comments and OIG Analysis

Management Comments: CBP concurred with Recommendation #10 [Develop and implement work/life balance programs that will promote staff retention at the NTC-P]. CBP said that subsequent to a Retention Study and Analysis completed in 2008, the National Targeting Center-Passenger implemented an active campaign to improve its retention rate and enhance its recruiting efforts. CBP said that at the request of the NTC-P, CBP-Human Resources Management (HRM) provided a report on Recruitment and Retention Strategies and provided recommendations to assist with these efforts. CBP said that the DHS 5-Step workforce planning model was used as a guide for the NTC-P as it continued its growth process. CBP said that in support of its Retention Study, the NTC-P conducted two internal surveys, in 2008 and 2009. CBP said that at the request of the NTC-P, HRM also completed independent exit surveys for the same years. CBP said that the Office of Field Operations Human Capital Division meets on a regular basis with NTC-P management to ensure that its staffing levels are maintained and that any recruitment issues are resolved expeditiously. CBP said that the study and surveys revealed a need to concentrate on the following: Job Satisfaction, Leadership and Management Knowledge, Employee Training, Quality of Life Concerns, Awards Performance, Employee Recognition, and Career Enhancement Opportunities. CBP said that as a result, the NTC-P implemented the following successful changes:

1. Improved its hiring processing and posting vacancy announcements
2. Implemented an Awards Recognition Day
3. Initiated an employee designed newsletter
4. Developed an Employee of the Month Program
5. Established permanent shifts with rotating long weekends
6. Established a permanent Training Team
7. Provided employees with multiple programs – e.g. IAP, ESTA, TSDB and Visa Revocation Unit, and Outbound for periodic rotations
8. Promoted external activities – e.g. Bring Your Child to Work Day, Combined Federal Campaign, blood drives, and food drives
9. Increased career ladder to the GS-13 level
10. Participated in the Student Career Experience

CBP said that since the NTC-P continues to grow in its responsibilities and staffing, the staff retention efforts remain one of its most important programs. CBP said that therefore, the NTC-P will continue to survey the staff on a yearly basis and implement changes that are within its control.

OIG Analysis: This recommendation is *resolved and open.* During the period of our review, we were aware that NTC-P had sought comments from current and former employees on work/life balance concerns, and had developed innovative programs such as those described above. During the period of our review, many had been suspended or curtailed because of staffing shortages. We request that CBP provide examples of the implementation of items 2, 4, 5, and 9. Evidence might include an agenda for item 2; a list of three recent Employee of The Month recipients for item 4; an assignment roster for a completed two-week period for item 5; and a position description and list of employees who have been promoted on the career ladder to a GS-13 for item 9. We commend the staff and management of the NTC-P for striving to identify and address work/life balance issues during a period of increasing workloads and limited resources.

Management Comments: CBP concurred with Recommendation #11 [Develop a program for career advancement within the NTC-P that includes necessary cross-training opportunities and a career ladder to better enable qualified analysts and targeting specialists to compete for advancement to senior analyst or supervisory positions]. CBP said that the Leadership Organization Development Division within CBP Office of Training and Development will work with the Office of Field Operations on this effort, to develop a CBP Succession Management System. CBP said that NTC-P staff will take a major role in defining jobs, competencies required, training and development needed to meet competency levels, and the means for assessing when a certain level of competence is achieved. CBP said that it is in the first phase of codifying the Succession Management procedures for senior leader and leader pools, and the next step will be to address supervisory and non-supervisory procedures during FY 2011. CBP said that the effort for all levels involves a significant amount of information from all CBP Assistant Commissioner offices, including the Steering Committee members who are the subject matter experts on the positions, experiences, and training required to hold those positions, and the experiences which indicate an individual will be competitive for his or her next job. CBP said that the Office of Training and Development will provide the templates for the information that must be collected and validated; program offices must complete the data collection and analysis.

OIG Analysis: This recommendation is *resolved and open.* CBP is requested to provide a summary on progress toward developing career development opportunities within the NTC-P. We commend CBP for its strategic vision for leadership development and succession.

Existing Small Scale Vetting and Interdiction Programs Are Effective and Merit Expansion

DHS has introduced several programs to improve information sharing on foreign nationals before they reach U.S. ports of entry. Two programs mandated by Congress, the ICE Visa Security Program and the CBP Immigration Advisory Program, are deployed to a limited number of locations. The USCG BASS initiative is a voluntary collaboration between the USCG, US-VISIT, CBP Border Patrol, and the United States Attorney's Offices in Puerto Rico and the Southern District of Florida. However, additional funding is required for expansion. These programs, which interdict dangerous and inadmissible foreign nationals before they reach the United States, merit additional resources.

ICE Visa Security Units Provide Investigative Expertise, But Deployment Overseas Is Slow

The legislatively mandated Visa Security Program assists the Department of State's effort to screen and vet visa applicants. The procedures ICE special agents use in visa security units to resolve a case are comparable to those used at the NTC-P. Evaluation of visa applicant information in DHS data systems is a complex process. It may be necessary to query multiple DHS data systems to resolve a case. An agent may need to review biometrics, information pertaining to previous U.S. arrivals and departures, immigrant benefit applications, prior interviews at ports of entry, immigration court records, and ongoing investigations. These records are stored in several different data systems. Access to fragmented DHS systems, and the specialized experience ICE special agents employ when they research and evaluate the data, strengthen the visa process.

Our 2008 report described some Department of State resistance to the visa security program and to the deployment of ICE agents overseas.[30] However, subsequent to that report, the Department of State has demonstrated an increased level of support. We observed one operational visa security unit in our overseas field work and visited another country where ICE opened a visa security unit in late 2010. ICE agents reported that consular officers now forward some cases to ICE for an opinion before they make a visa decision, and rely more on ICE to screen and vet visa applications overseas.

Although the program provides an additional tool to secure the visa process, visa security unit deployment overseas has been slow. ICE has established visa security units at only 19 of the 57 high-risk posts identified through risk analysis and consultations with the Department of State.[31] Funding constraints and the complex process to obtain approval for additional overseas DHS staff will slow further expansion.

The deployment of visa security units overseas has been a challenge, but ICE has introduced technologies and procedures that enable agents to screen and vet some applications at ICE headquarters. In February 2010, ICE launched web-based Visa Security Program tracking software that enables headquarters to track fieldwork and assign cases worldwide. The Visa Security Program has agents at headquarters who review security advisory opinions, which are third agency checks the Department of State requests on a small number of visa applications with security implications. Shared data systems at the NTC-P allow the Visa Security Program liaison to share information on security advisory opinion cases. When systems malfunction at an embassy and another field office cannot cover the workload, the Visa Security Program at headquarters has the technology to provide some backup.

[30] DHS OIG, *U.S. Immigration and Customs Enforcement Visa Security Program*, OIG-08-79, July 2008, pp. 20–21.

[31] Riyadh, Saudi Arabia (2003), Dhahran, Saudi Arabia (2003), Abu Dhabi, United Arab Emirates (2005), Dubai, United Arab Emirates (2005), Islamabad, Pakistan (2005), Manila, Philippines (2005), Cairo, Egypt (2007), Caracas, Venezuela (2007), Montreal, Canada (2007), Hong Kong, SAR (2007), Casablanca, Morocco (2008), Frankfurt, Germany (2008), Amman, Jordan (2009), and Jakarta, Indonesia (2009). An office in Jeddah, Saudi Arabia, was closed in 2005 but re-opened in February 2010. London, United Kingdom, Tel Aviv, Israel, Sanaa, Yemen, and Jerusalem were added in 2010, after we completed our fieldwork.

This capability could be used to expand international coverage for the Visa Security Program. When DHS and the Department of State agree to establish a new visa security unit overseas, it can take months to arrange the overseas deployment. During this period, some of the ICE agents scheduled to be deployed should work in the Visa Security Program headquarters to screen and vet applicants from the newly designated country's caseload. At the request of the Department of State, ICE agents should screen applicants from some of the other countries designated high-risk posts where ICE will not be able to establish a visa security unit in the near future. The agents should provide backup to field offices when there are system malfunctions or unusually high volumes of applications. The Visa Security Program headquarters support element would not provide all the functionality of a Visa Security Program in an embassy or consulate overseas. The ICE agent would not have access to original documents or the informal face-to-face exchange with consular officers. However, the headquarters support element could address some risks at posts without a visa security unit.

Recommendation

We recommend that U.S. Immigration and Customs Enforcement:

Recommendation #12: Establish a Visa Security Program headquarters support element to screen and vet visa applications for: 1) consular posts already designated for future visa security unit expansion; 2) high-risk consular posts where expansion is not imminent; and 3) Visa Security Units experiencing technical difficulties.

While a Valuable Asset, the Immigration Advisory Program Is Not at Its Full Potential

The CBP Immigration Advisory Program is a valuable counterterrorism, law enforcement, and facilitation asset for DHS, foreign partners and airlines. IAP officers intercept high-risk passengers who seek to board flights to the United States. Officers also monitor airport security and observe and talk to passengers bound for the United States, and observe airport authorities as they conduct security checks and baggage searches. When time permits, officers assist foreign nationals to resolve ESTA application issues or assist airlines that cannot locate approvals in the airline system. Officers may also assist legitimate travelers who have lost documents, which reduces the caseloads of consular officers and DHS staff who would otherwise need to draft transportation letters.

The IAP does not operate at its full potential. Federal law requires CBP to identify 50 locations for expansion. Negotiations are ongoing to place officers at additional airports. As with the Visa Security Units, the complex process to obtain approval for additional overseas assignment of DHS staff slows the addition of Immigration Advisory Program officers. CBP has deployed officers to 10 airports in eight countries for the IAP. In the locations we visited, the teams were understaffed for the expanded workload that resulted from the December 2009 bombing attempt. Additions to the TSDB watch list and State Department visa revocations require resolution of more possible hits. Officers are asked to interview more U.S. citizens and permanent residents to determine whether they should be allowed to board and to obtain information on prior travel. With the introduction of mandatory ESTA applications in January 2010, the need to resolve inappropriate ESTA denials has grown.

Additional IAP resources are needed because of the large number of departure gates at major international airports, the distances between those gates, the number of departures from the busier airports, and the need to station an officer at the gate to observe passengers in the event of a no-fly case. Officers must prioritize cases without full information. For example, they must often decide between a possible match to a TSDB hit and a likely match involving a visa revocation.

IAP team leaders start their days by reviewing possible NTC-P matches before leaving home. While working in the airport, officers have limited access to DHS computer systems and databases. Data entry may not be completed until after the last flights have departed and they have returned home. Team leads remain on call overnight, on weekends, and when on leave locally. Two of the four IAP teams we visited operated with 6-month TDY staff. Even with experienced temporary officers, the teams can find it difficult to establish and maintain working relationships with local security officials.

At each of the four sites we reviewed, the program would benefit from at least one additional permanent or TDY CBP officer. This would provide more backup for team leads, allow teams to better manage multiple simultaneous hits, expand screening interviews, and improve liaison with local officials. It would also enable CBP to assist legitimate travelers to resolve document problems when asked by the local consulate, host government, or airline. Officers currently have time to take on only a few such cases a day.

With expanded support for ESTA applicants, the IAP might fund staff to assist with ESTA applications, which would also provide a surge capacity for resolving terrorist and criminal cases. Officials from three of the four IAP sites we reviewed said there were more ESTA cases than current staff could manage. The *Implementing Recommendations of the 9/11 Commission Act of 2007*, which established ESTA, permits CBP to collect fees, set at a level that will ensure recovery of the full costs of providing and administering the system. Soon CBP will need to transition to a fee-based structure for ESTA.[32] Assisting with ESTA cases is one IAP responsibility, and CBP should consider whether ESTA fees might fund some additional IAP positions.

Recommendation

We recommend that U.S. Customs and Border Protection:

Recommendation #13: Assess and report on the feasibility of using Electronic System for Travel Authorization fees to fund some Immigration Advisory Program positions in airports from which visa waiver nationals depart.

Connectivity Issues Hamper the USCG BASS

The BASS represents an innovative information-sharing venture by the USCG and US-VISIT. If the identity, nationality and potential security or criminal threat of an interdicted person could be positively established at sea, it would be possible to make informed decisions about which migrants to bring to U.S. territory. Specifically, the USCG would bring only those migrants who needed international protection or whom the U.S. Attorney's Office agreed to prosecute as criminals, smugglers, or repeat offenders. While biometric technology is central to the success of this program, cooperation between federal agencies and with the migrants' countries of origin, is also essential.

[32] A fee of $14 for each ESTA application was introduced in September 2010, after field work was completed for this report.

BASS uses a hand-held biometric device that records two fingerprints and a photograph; a computer to process the fingerprints; a second computer to transmit the encrypted data to shore; and maritime satellite communications service to transmit the data. The transmitted fingerprints are compared to biometrics already stored in IDENT and any new identities are enrolled. As our inspectors observed during a visit to a cutter, biometric enrollment is a difficult, time-consuming process. The USCG usually works in rough seas as it transfers migrants from their flimsy seacraft onto the cutter while simultaneously maintaining order, providing food and medical assistance to the migrants, and operating delicate and slow BASS equipment. When the BASS equipment works properly and there are about 40 migrants on board, it can take 24 hours to process biometric enrollments, transmit data, and determine which migrants will be prosecuted or repatriated. Conditions are not usually optimal. Under adverse conditions, it can take 2 to 3 days to process 40 migrants. Crewmembers who process biometric enrollment of migrants often work around the clock until data transmission is completed and return with little rest to perform other duties.

Using biometrics acquired at sea to identify potentially dangerous aliens or aliens who have repeatedly attempted to enter the US for criminal prosecution, has proven to be an effective deterrent to maritime migration. However, on our site visit to Puerto Rico we noted several challenges that seriously hinder efficiency, such as outdated or insufficient technology. For example, the most significant challenge for the BASS is the timely transfer of biometric information to IDENT to avoid unduly prolonging the period migrants are held at sea for processing. The primary data link on USCG cutters utilizes maritime satellite communications. The existing equipment has a transmission speed of about 64 kilobits per second. USCG crews reported the transmission of biometric data is inconsistent due to the erratic speed of service. When connectivity is sporadic, transmission of data can take 6 to 7 hours and in rare cases 24 hours. If the system malfunctions, the biometric crew must re-fingerprint migrants and then process and retransmit the biometric data. USCG officials said that a contract was submitted for upgrading to a faster satellite communications service, but problems with the contract and availability of funds delayed the upgrade.

The two-print hand-held device that collects biometric information is not optimal for maritime conditions, as migrants intercepted at sea may be dehydrated, or their fingers may have been immersed in sea water, which can make it more difficult to collect two good readable fingerprints. With 10 prints, the chances of matching prints to an existing IDENT record increases. Additionally, the data from portable two-print devices may not match latent fingerprints from crime scenes. However, the USCG cannot switch to portable ten-print devices because the satellite service does not have sufficient bandwidth.

Moreover, USCG cutters that operate off the eastern coast of Puerto Rico do not have satellite communication equipment. After they collect data from interdicted migrants, the cutters return to shore to transmit the information. The USCG must decide whether to bring an interdicted migrant onto U.S. territory or lose custody when it does not know what information is available in DHS databases. Given that the caseload off the eastern coast of Puerto Rico is more varied than the largely Dominican population interdicted on the western shore, the USCG may miss the opportunity to detain migrants who pose a serious risk to the United States.

Although the USCG captures and transmits fewer biometrics off the coast of south Florida, operable satellite communication is essential in this area as well. USCIS refugee officers conduct protection screening interviews for interdicted migrants on the cutters at sea. The officers use USCG satellite communication to transmit their preliminary protection decisions to USCIS headquarters for review. There are frequently delays in the transmission of data, in some cases for more than eight hours, which can slow migrant processing.

Recommendation

We recommend that the U.S. Coast Guard:

Recommendation #14: Upgrade current maritime satellite communication equipment to provide high-speed transmission capabilities. This would enable cutters that interdict migrants to conduct 10-print biometric enrollment.

Management Comments and OIG Analysis

Management Comments: ICE concurred with Recommendation #12 [Establish a Visa Security Program headquarters support element to screen and vet visa applications for: 1) consular posts already designated for future visa security unit expansion; 2) high-risk consular posts where expansion is not imminent; and 3) Visa Security Units experiencing technical difficulties]. ICE stated that the Visa Security Program has established a Security Advisory Opinion Unit which serves as the headquarters support element. ICE stated that the unit does conduct screening and vetting of consular posts designated for future expansion and provides support to overseas ICE Attaché offices conducting visa security operations when they have technical difficulties. ICE stated that the Security Advisory Opinion Unit supports all consular issuing posts worldwide and expects to add two additional analysts in January 2011. Additionally, ICE stated that it is pursuing cooperation from the Department of State and Customs and Border Protection for the enhancement of existing technologies to increase the efficiency of screening and vetting operations. ICE stated that it strongly believes that conducting operations remotely is not a substitute for deploying ICE Special Agents to consular issuing posts to work cooperatively with Department of State personnel issuing visas and feels this is required in order to fulfill its mandate in the Homeland Security Act of 2002.

OIG Analysis: This recommendation is *resolved and open.* We agree that deploying Special Agents to the field is preferable to relying solely on the headquarters unit, when funding and logistics permit. We request ICE provide an update on the level of increased coverage by the headquarters Security Advisory Opinion Unit.

Management Comments: CBP concurred with Recommendation #13 [Assess and report on the feasibility of using ESTA fees to fund some Immigration Advisory Program positions in airports from which visa waiver nationals depart]. CBP stated that the ESTA fee must ensure recovery of the full costs of providing and administering the system. CBP said that the ESTA fee statute was written narrowly in scope with strict limitations that prevent CBP from recovering excess money. CBP said that in developing the ESTA fee, CBP evaluated many different costs and completed an extensive fee analysis to determine what costs could be included in the fee. CBP said that the analysis was submitted to the Office of Management and Budget who reduced the proposed fee amount before approving. CBP said that it will consult with the Office of Chief Counsel to determine the feasibility of funding Immigration Advisory Program positions.

OIG Analysis: This recommendation is *resolved and open*. We request a report on the outcome of the consultation with the Office of Chief Counsel. We recognize that CBP must comply with legal interpretations of the statute and regulations, and that in any event ESTA fees would fund only a portion of Immigration Advisory Program positions, as ESTA passengers represent only a portion of their duties. We will close this recommendation based on CBP's efforts rather than on a specific outcome.

Management Comments: The USCG concurred with Recommendations #14 [Upgrade current maritime satellite communication equipment to provide high-speed transmission capabilities. This would enable cutters that interdict migrants to conduct 10-print biometric enrollment]. The USCG said that it is assessing means to improve cutter connectivity and bandwidth for segments of the cutter fleet to include BASS-equipped units. The USCG said that BASS meets the DHS standard for two-print collection.

OIG Analysis: This recommendation is *resolved and open*. The DHS minimum standard for print collection is two prints, but ten-print collection is widely employed across the Department of Defense, Department of Justice, and DHS. USCG should provide an update on the USCG's assessment of the means to improve connectivity and bandwidth for segments of the cutter fleet. We recognize that funding constraints may affect implementation.

DHS Officers Need Assistance Navigating Fragmented Data Systems

Data System Shortfalls Impede Overseas Officer Effectiveness

To determine whether foreign nationals represent a terrorist or criminal threat, or are eligible for an immigration benefit, DHS officers abroad routinely use more than 17 data management systems. A single sign-on to these systems would improve productivity and accuracy. Most of the officers we interviewed overseas said each DHS data system requires a unique username and password. Usernames vary from assigned codes to email addresses, and passwords require letters, numbers, and symbols in different sequences. Users need to manage multiple usernames and passwords to log onto the various systems. Expiration cycles for passwords vary from 30 to 90 days, and infrequent use of systems with short password cycles often means users are locked out of databases. When users are locked out of databases, it may require written authorization from a regional office or headquarters to reinstate a lapsed password, which creates a delay.

In the overseas environment, it is often necessary to log off of one data system to log onto another, which—coupled with automatic log-offs of open systems after 15 to 20 minutes for security purposes—makes checks in multiple systems a time-consuming process. Some officers whose passwords have lapsed ask their DHS colleagues to conduct searches for them.

The productivity cost of multiple passwords is difficult to calculate. Some officers said they cumulatively spend several hours a week logging into and out of data systems, and most officers conduct searches on behalf of colleagues. Because it is difficult to check across systems, a more serious potential outcome is that an officer might not consider all available information on a case that initially appears straightforward. The Office of the Chief Information Officer confirmed that a single sign-on for the data systems used by multiple DHS components is feasible and would not constitute a security risk. While overseas officers may have the greatest difficulty managing multiple passwords and expiration cycles, a single sign-on would also benefit officers domestically.

The DHS systems most widely used by multiple components overseas include the following:

- ADIS
- ATS-P
- ESTA
- ENFORCE / Enforce Alien Removal Module (EARM)
- IDENT
- Intel Fusion / Avalanche
- ISRS
- SEVIS
- TECS (including data fields formerly known as the Interagency Border Inspection System, or IBIS)
- CIS, CLAIMS3, Computer Linked Application Information Management System 4 (CLAIMS4), Refugees, Asylum, and Parole System (RAPS)

DHS officers who were familiar with the full range of available data systems also reported that it was difficult to navigate the many web-based systems used to track foreign nationals. There is currently no consolidated access to the web-based DHS data systems. Officers must obtain web addresses individually from several offices within each component. A single portal on the DHS intranet, the secure Homeland Security Information Network (HSIN), would improve efficiency through consolidated access to web-based systems.

A single intranet portal would resolve only some of the challenges inherent in the DHS systems. Many key databases, such as TECS and CIS, predate today's internet architecture, and may not be adaptable for intranet use. However, a single web-based portal could be used to consolidate information for users on what data systems exist and how authorized users can obtain access. Several officers overseas reported they learned of valuable systems or useful search capabilities only through word of mouth or were uncertain of the capabilities of systems they did not use.

The DHS web-based systems that could be consolidated on a single intranet portal include the following:

- ADIS
- ATS-P
- ESTA
- ENFORCE / EARM
- IDENT
- Intel Fusion / Avalanche
- ISRS
- SEVIS

DHS officers reported they sometimes lacked confidence that their searches had in fact yielded all of the accurate, current information in DHS databases. We were told that users need to be aware of the structures of the databases, what information is captured for what purpose, and whether the accuracy of some search results needs to be verified against other sources. While NTC-P targeting specialists knew the limitations of the data they used, many overseas officers said they did not have enough training and experience on the systems, and they addressed a wider range of issues than what NTC-P targeting specialists address. For example, responsibility for the issuance of transportation letters shifts among CBP, ICE, and USCIS, to address workload needs. CBP and ICE attachés may need to provide current travel and immigration information to local law enforcement to support a joint investigation.

There is a headquarters initiative underway that could be adapted to address this need. In November 2009, the department initiated a Bottom Up Review which, among other accomplishments, recommends creating an integrated departmental Information Sharing Architecture to consolidate and streamline access to intelligence, law enforcement, screening, and other information across the department.[33] To address screening requirements, the department identified the need for a Controlled Homeland Information Sharing Environment to strengthen information sharing on person-centric data. Planning toward this goal includes the Screening Coordination Office, the Office of the Chief Information Officer, and Intelligence and Analysis, as well as representatives from the Privacy Office and the Office of the General Counsel, and coordinates through the Information Sharing Governance Board.

Recommendations

We recommend that the Office of the Chief Information Officer:

Recommendation #15: Enable officers and analysts to use a single sign-on for DHS systems used for screening foreign nationals.

Recommendation #16: Provide additional resources to establish a portal on the secure Homeland Security Information Network through which authorized DHS users can log on to DHS web-based databases to access information on foreign nationals.

We recommend that the Office of Policy Screening Coordination Office:

Recommendation #17: Provide additional personnel for the Controlled Homeland Information Sharing Environment, which supports the Bottom Up Review Initiative for a DHS Integrated Information Sharing Architecture. This initiative would assist authorized users in navigating DHS data systems to access information on foreign nationals.

[33] http://www.dhs.gov/xlibrary/assets/bur_bottom_up_review.pdf

Overseas DHS Officers Require Additional Training on Immigration Enforcement and Benefits

DHS overseas staff is expected to understand more of the process by which DHS tracks and evaluates foreign nationals than their domestic counterparts. The State Department and host governments routinely ask overseas staff questions about all DHS functions. However, some officers have limited immigration backgrounds or experience and minimal pre-deployment training on DHS data systems. Insufficient knowledge of immigration issues and operational challenges with DHS data systems make it difficult to screen and process cases, and limit the ability to share valuable information. In most offices we visited overseas, officers with an immigration background provided informal assistance to many of their colleagues. Officers with experience using legacy systems such as TECS, CIS, CLAIMS3, and EARM conducted research to assist colleagues. While this practice demonstrates a commitment to information sharing, it also has a negative effect on productivity. In addition, many officers commented that they did not know what all of the relevant DHS data systems were.

The Office of Policy, Office of International Affairs, has recognized that Department of State consular officers and host governments expect DHS officers overseas to be able to answer a broad range of questions about DHS operations. With the exception of legacy immigration officers, most USCIS, ICE, and CBP officers have been trained on either immigration benefits or immigration enforcement, but not both. USCG International Port Security Liaison Officers and International Training Team members are not trained in all areas of immigration law, but are asked for information by host governments they work with in the maritime domain. TSA officers and senior legacy customs service officers in CBP and ICE may not have ever received formal training on immigration benefits or enforcement. The Office of International Affairs concluded that DHS should provide its overseas staff with cross-component training. In its International Strategic Framework, the Office of International Affairs identified providing the necessary skills, knowledge, and training to effectively carry out DHS international activities as objectives for DHS overseas employees. Cross-training on immigration enforcement and benefits would contribute to productivity. Training on how to use data systems to obtain accurate, current information on foreign nationals could improve efficiency. Training staff from CBP, the USCG, ICE, and USCIS may be able to assist in the development of an overseas training using materials developed for domestic officers, or may be able to provide subject matter expertise.

Recommendation

We recommend that the Office of Policy Office of International Affairs:

Recommendation #18: In consultation with training staff from CBP, ICE, and USCIS, develop training designed to provide an overview for overseas DHS officers on immigration law, DHS and other federal government programs, policies and procedures related to foreign nationals, and DHS and other federal data systems that house information on foreign nationals.

Management Comments and OIG Analysis

Management Comments: CIO concurred with Recommendation #15 [Enable officers and analysts to use a single sign-on for DHS systems used for screening foreign nationals]. CIO said that it generally agreed with the intent of the recommendations as a means to improve the effectiveness of Information Sharing on Foreign Nationals. CIO said that a change to the text would provide additional clarity, and suggested that the text read "Provide additional resources to make available the enterprise single sign on capability that enables officers and analysts to use a single sign-on for the DHS systems used for screening foreign nationals."

OIG Analysis: This recommendation is *resolved and open.* We read the CIO comment to mean that it agrees with the intent of this recommendation, but will need additional resources. Providing a single sign on would improve productivity for thousands of DHS employees. When CBP Officers have less than 30 minutes to determine whom to board, a single sign on may help avoid costs associated with allowing inadmissible aliens to board. To close this recommendation, please provide a detailed estimate of the resources necessary to provide single sign on capability. Please also provide a copy of the CIO budget request and justification for additional resources for implementing single sign on by October 31, 2011.

Management Comments: CIO concurred with Recommendation #16 [Provide additional resources to establish a portal on the secure HSIN through which authorized DHS users can log on to

DHS web-based databases to access information on foreign nationals]. CIO said that it generally agreed with the intent of the recommendations as a means to improve the effectiveness of Information Sharing on Foreign Nationals. CIO said that a change to the text would provide additional clarity, and suggested that the text read, “Provide additional resources to establish a capability on the DHS HSIN through which authorized DHS users can discover information on how to obtain access and log on to DHS web-based databases to access information on foreign nationals.”

OIG Analysis: This recommendation is *resolved and open.* We read the CIO comment to mean that while it agrees with the intent of this recommendation, it would need additional resources. Establishing a portal on the DHS HSIN would improve productivity for thousands of DHS employees. To close this recommendation, please provide a detailed estimate of the resources necessary to establish a portal. Please also provide a copy of the CIO budget request and justification for additional resources for implementing single sign on.

Management Comments: The Office of Policy concurred with Recommendation #17 [Provide additional personnel for the Controlled Homeland Information Sharing Environment, which supports the Bottom Up Review Initiative for a DHS Integrated Information Sharing Architecture. This initiative would assist authorized users in navigating DHS data systems to access information on foreign nationals]. The Office of Policy stated that during the next budget request cycle, it will request additional personnel for the Controlled Homeland Information Sharing Environment.

OIG Analysis: This recommendation is *resolved and open*. Upgrading the Controlled Homeland Information Sharing Environment would improve productivity for thousands of DHS employees. Please provide a copy of the Office of Policy budget request and justification for additional personnel for the Controlled Homeland Information Sharing Environment.

Management Comments: The Office of Policy concurred with Recommendation #18 [In consultation with training staff from CBP, ICE, and USCIS, develop training designed to provide an overview for overseas DHS officers on immigration law, DHS and other federal government programs, policies and procedures related to foreign nationals, and DHS and other federal data systems that house information on foreign nationals]. The Office of Policy stated that since April 5, 2010, this initiative has been integrated into the DHS International Strategic Framework. The Office of Policy provided written guidance under the Homeland Security Priority – "Maturing and Unifying the Department," Objective 5.5 states – "Provide DHS employees with the necessary skills, knowledge, and training to effectively carry out DHS international activities."

The Office of Policy also stated that DHS is engaged in ongoing efforts to enhance the capabilities of DHS personnel serving in any capacity overseas including the establishment of a standard course of instruction that would provide an overview of the multiple DHS international programs, policies, operations, systems and capabilities that they would need to know about or would encounter overseas. The Office of Policy stated a key feature would be to provide resources for staff, before they are assigned overseas, to include protocols, procedures, current issues, and perhaps most importantly direct contact for information.

The Office of Policy advised that the Federal Law Enforcement Training Center (FLETC) is now developing a standard DHS international pre-deployment training course that will combine both the security considerations for DHS officials operating overseas and information regarding the DHS roles and missions internationally that will provide the individual a good foundation of the broad scope of DHS international work. FLETC will continue to consult with DHS as they progress to meet this requirement.

OIG Analysis: This recommendation is *resolved and open*. Please provide the draft or final training and guidance provided to DHS staff overseas. Please also provide status reports which include evidence of consultation with training officers at CBP, ICE, and USCIS regarding requirements of the training course, and any additional training development initiatives provided by FLETC regarding the DHS international pre-deployment training course.

Appendix A
Purpose, Scope and Methodology

We initiated this review to evaluate how biographic and biometric information is shared among DHS components. We focused our review on:

- How components check and evaluate information;
- The timeliness and thoroughness of information sharing;
- The strengths and weaknesses of current information-sharing procedures;
- What plans exist to consolidate information and improve data analysis; and
- What short-term solutions might be implemented to improve information sharing.

This is the first of a series of reports that will discuss information sharing. Although some of our recommendations cover all DHS information-sharing programs, we limited the scope of this report to initiatives to screen foreign nationals while they are still overseas. Additional reports will examine information sharing on foreign nationals at the border and in domestic programs. Our scope was limited to programs that evaluate foreign nationals. We did not review measures for U.S. citizens, except for travel screening programs that cover all passengers. We also did not evaluate programs that provide physical security overseas nor did we review cargo screening. We did not focus on privacy, civil rights, and civil liberties, or redress aspects of the systems or processes under review. Although the focus of this review was on overseas operations, some recommendations were written to improve all DHS information-sharing programs.

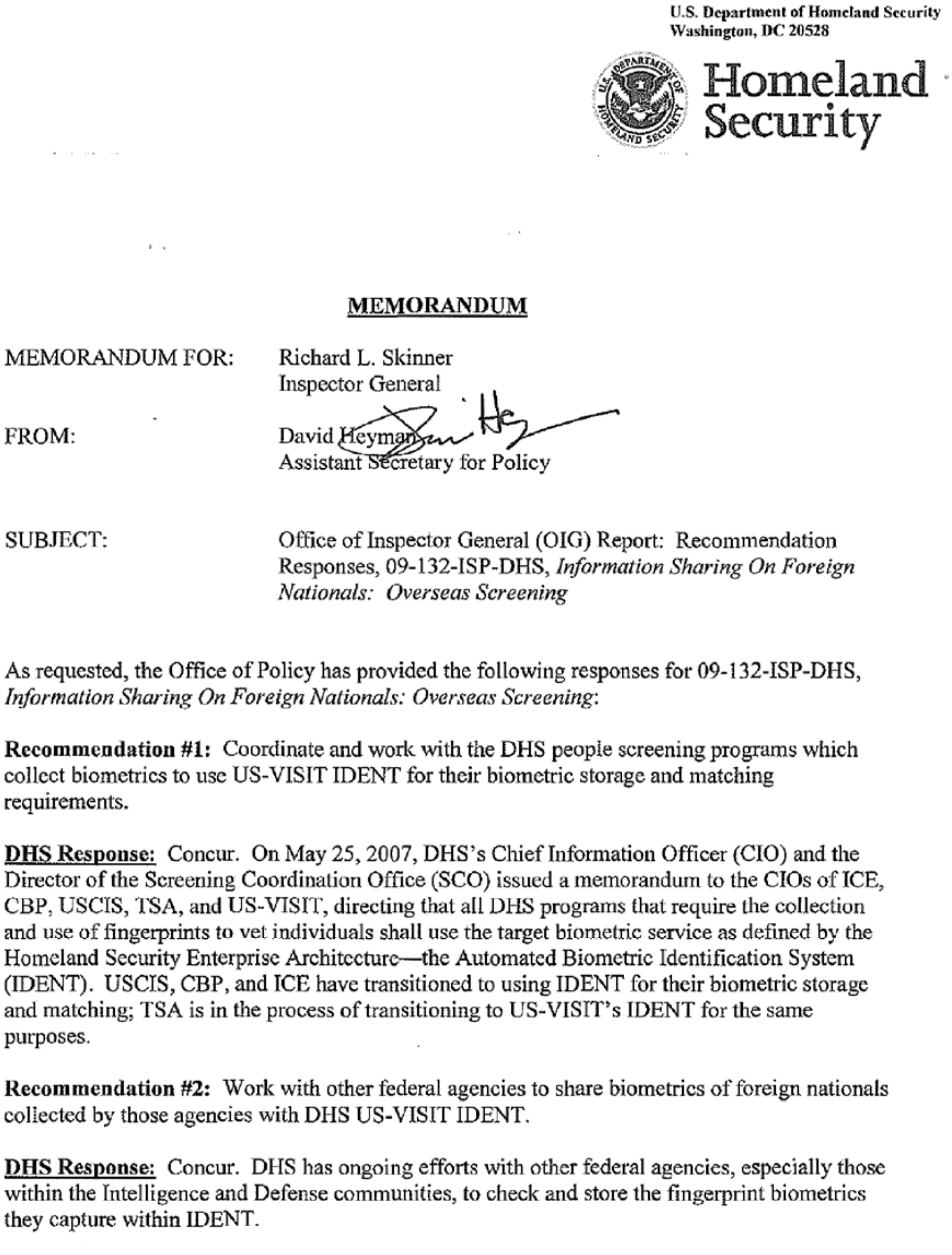
We conducted fieldwork for this report from February to June 2010. We conducted 110 individual and group interviews, which included 250 DHS personnel. We interviewed personnel from five operational components: CBP, ICE, TSA, the USCG, and USCIS. We determined that TSA employees who work in DHS offices overseas did not play a significant role in information sharing on foreign nationals at the time of our fieldwork, but may do so after Secure Flight is fully operational on international flights after December 2010. We interviewed personnel from several headquarters support offices, including the Office of Policy Screening Coordination Office and Office of International Affairs; Office of Intelligence and Analysis Border and Immigration Analysis Division, Information Sharing and Collaboration Branch and National Immigration Information Sharing Office; US-VISIT;

the Office of Management Office of the Chief Information Officer; and the Counterterrorism Section in the Office of Operations Coordination and Planning. We interviewed experts from several of the major DHS data systems, including US-VISIT, TECS, ATS-P, ESTA, ENFORCE, SEVIS, ICE Pattern Analysis and Information Collection System (ICE-PIC), CIS, USCIS immigration tracking systems, and the USCIS planned upgrade, Transformation. We reviewed documentation provided by DHS components and viewed many data system demonstrations.

We conducted site visits to DHS offices in Dublin, Ireland; London, United Kingdom; Rome, Italy; The Hague, The Netherlands; Athens, Greece; Frankfurt, Germany; and Warsaw, Poland. Those sites included four Immigration Advisory Program locations, four USCIS field offices, five TSA offices, one established and one planned visa security unit, and preclearance operations in one location. We also interviewed CBP and ICE officers at some embassies and consulates, including ICE agents who conduct investigations involving foreign nationals and CBP officers who issue transportation letters. Our site visits included five established Visa Waiver Program countries, one country (Greece) that recently became a visa waiver country, and one country (Poland) without visa waivers. Because the Icelandic volcano eruptions affected our travel, we interviewed the Immigration Advisory Program officers who cover Schiphol Airport while the airport was closed. Additionally, we interviewed DHS officers in Frankfurt by telephone from DHS offices in The Netherlands. After flights resumed, we traveled to Frankfurt for a short in-person review of data systems.

OIG inspectors observed NTC-P staff for one week in March 2010 and conducted a follow-up visit in May 2010. We observed the USCG migrant interdiction program, which included the use of USCG cutters and search and rescue helicopters, in Puerto Rico in April 2010. We also conducted site visits to the Regional Carrier Liaison Group at Miami International Airport in Florida in April 2010, and at John F. Kennedy International Airport in New York in May 2010.

This review was conducted under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections* issued by the President’s Council on Integrity and Efficiency.



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

Homeland
Security

MEMORANDUM

MEMORANDUM FOR: Richard L. Skinner
Inspector General

FROM: David Heyman
Assistant Secretary for Policy

SUBJECT: Office of Inspector General (OIG) Report: Recommendation Responses, 09-132-ISP-DHS, *Information Sharing On Foreign Nationals: Overseas Screening*

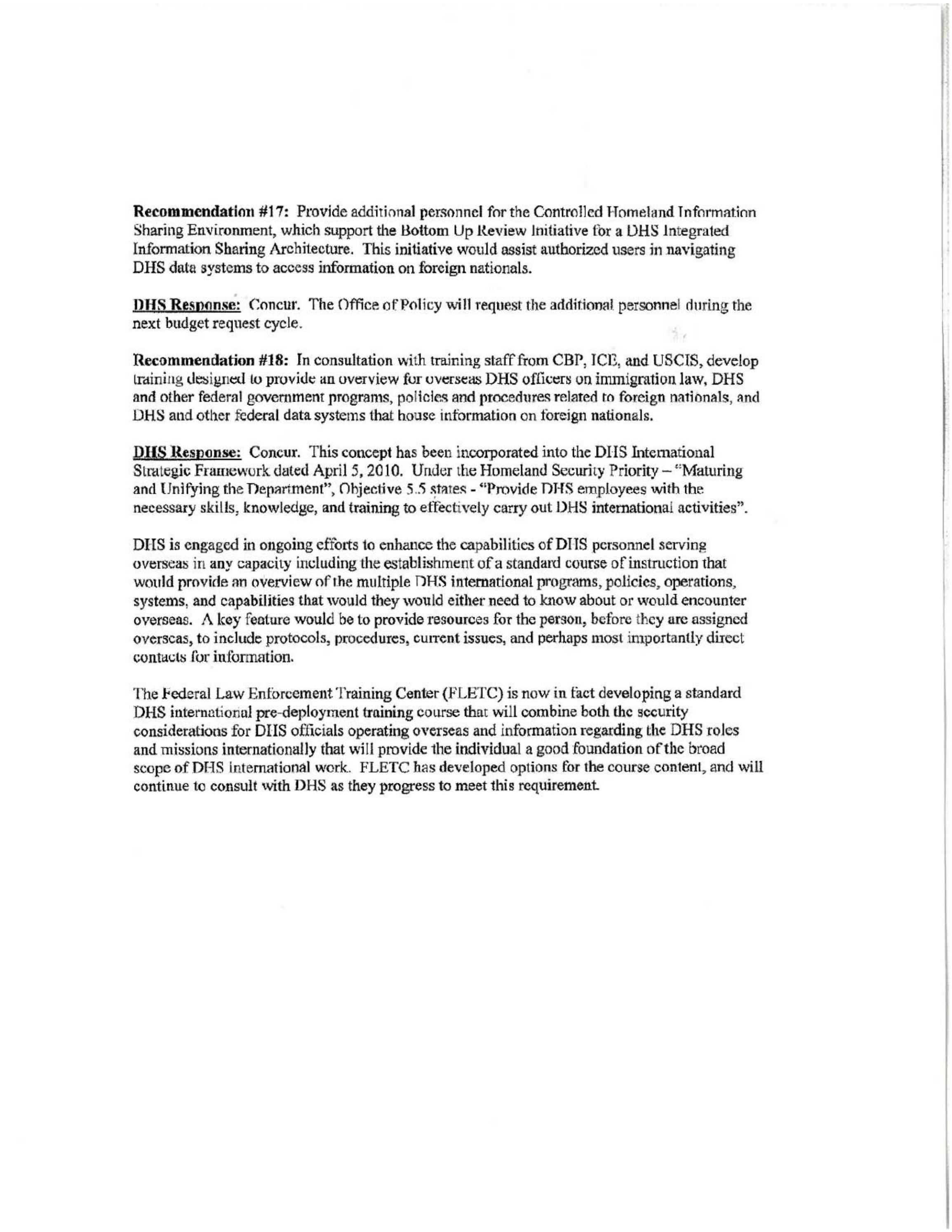
As requested, the Office of Policy has provided the following responses for 09-132-ISP-DHS, *Information Sharing On Foreign Nationals: Overseas Screening*:

Recommendation #1: Coordinate and work with the DHS people screening programs which collect biometrics to use US-VISIT IDENT for their biometric storage and matching requirements.

DHS Response: Concur. On May 25, 2007, DHS's Chief Information Officer (CIO) and the Director of the Screening Coordination Office (SCO) issued a memorandum to the CIOs of ICE, CBP, USCIS, TSA, and US-VISIT, directing that all DHS programs that require the collection and use of fingerprints to vet individuals shall use the target biometric service as defined by the Homeland Security Enterprise Architecture—the Automated Biometric Identification System (IDENT). USCIS, CBP, and ICE have transitioned to using IDENT for their biometric storage and matching; TSA is in the process of transitioning to US-VISIT's IDENT for the same purposes.

Recommendation #2: Work with other federal agencies to share biometrics of foreign nationals collected by those agencies with DHS US-VISIT IDENT.

DHS Response: Concur. DHS has ongoing efforts with other federal agencies, especially those within the Intelligence and Defense communities, to check and store the fingerprint biometrics they capture within IDENT.



Recommendation #17: Provide additional personnel for the Controlled Homeland Information Sharing Environment, which support the Bottom Up Review Initiative for a DHS Integrated Information Sharing Architecture. This initiative would assist authorized users in navigating DHS data systems to access information on foreign nationals.

DHS Response: Concur. The Office of Policy will request the additional personnel during the next budget request cycle.

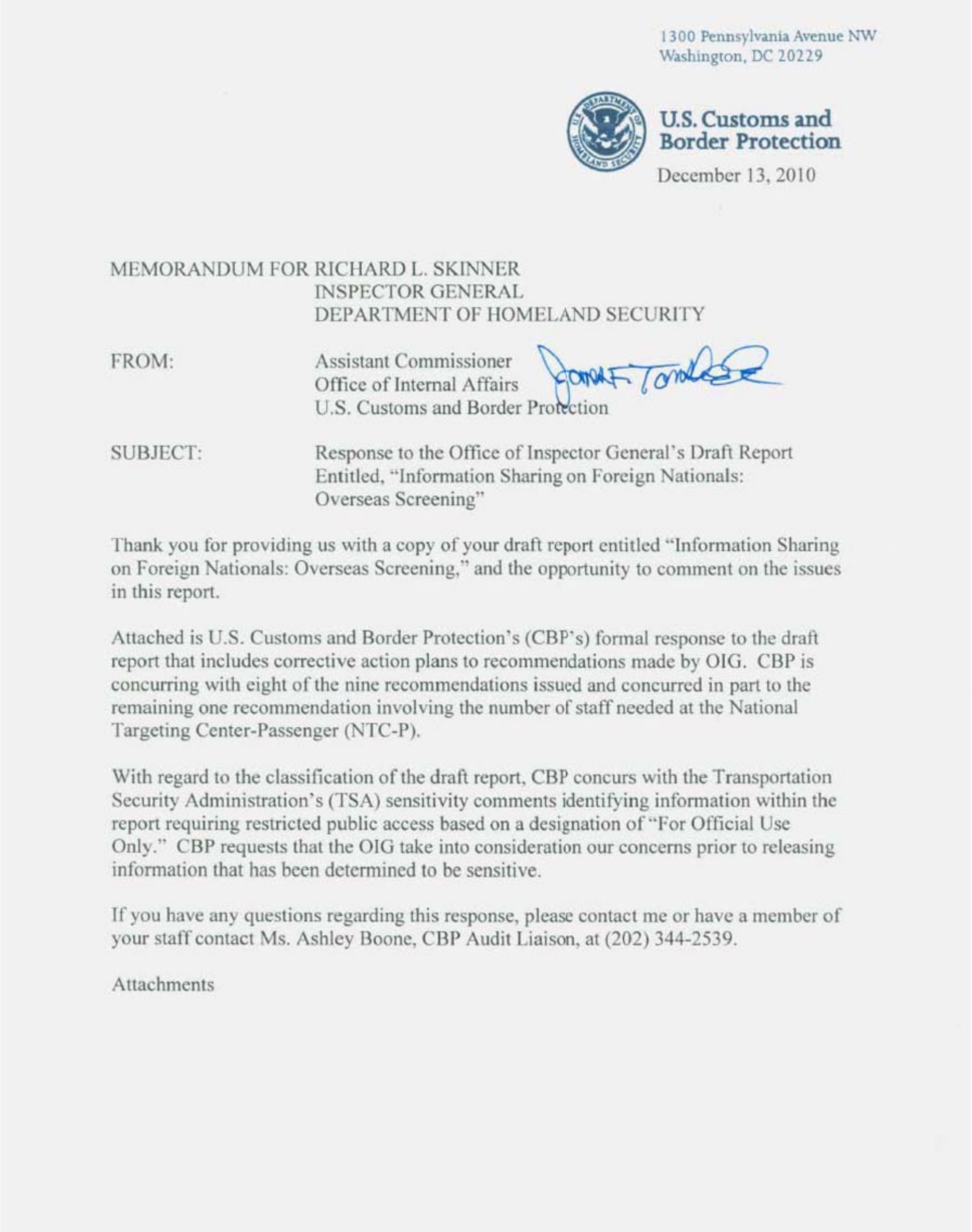
Recommendation #18: In consultation with training staff from CBP, ICE, and USCIS, develop training designed to provide an overview for overseas DHS officers on immigration law, DHS and other federal government programs, policies and procedures related to foreign nationals, and DHS and other federal data systems that house information on foreign nationals.

DHS Response: Concur. This concept has been incorporated into the DHS International Strategic Framework dated April 5, 2010. Under the Homeland Security Priority – "Maturing and Unifying the Department", Objective 5.5 states - "Provide DHS employees with the necessary skills, knowledge, and training to effectively carry out DHS international activities".

DHS is engaged in ongoing efforts to enhance the capabilities of DHS personnel serving overseas in any capacity including the establishment of a standard course of instruction that would provide an overview of the multiple DHS international programs, policies, operations, systems, and capabilities that would they would either need to know about or would encounter overseas. A key feature would be to provide resources for the person, before they are assigned overseas, to include protocols, procedures, current issues, and perhaps most importantly direct contacts for information.

The Federal Law Enforcement Training Center (FLETC) is now in fact developing a standard DHS international pre-deployment training course that will combine both the security considerations for DHS officials operating overseas and information regarding the DHS roles and missions internationally that will provide the individual a good foundation of the broad scope of DHS international work. FLETC has developed options for the course content, and will continue to consult with DHS as they progress to meet this requirement.

Appendix B
Management Comments to the Draft Report



1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and
Border Protection

December 13, 2010

MEMORANDUM FOR RICHARD L. SKINNER
INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

FROM: Assistant Commissioner
Office of Internal Affairs
U.S. Customs and Border Protection

SUBJECT: Response to the Office of Inspector General's Draft Report
Entitled, "Information Sharing on Foreign Nationals:
Overseas Screening"

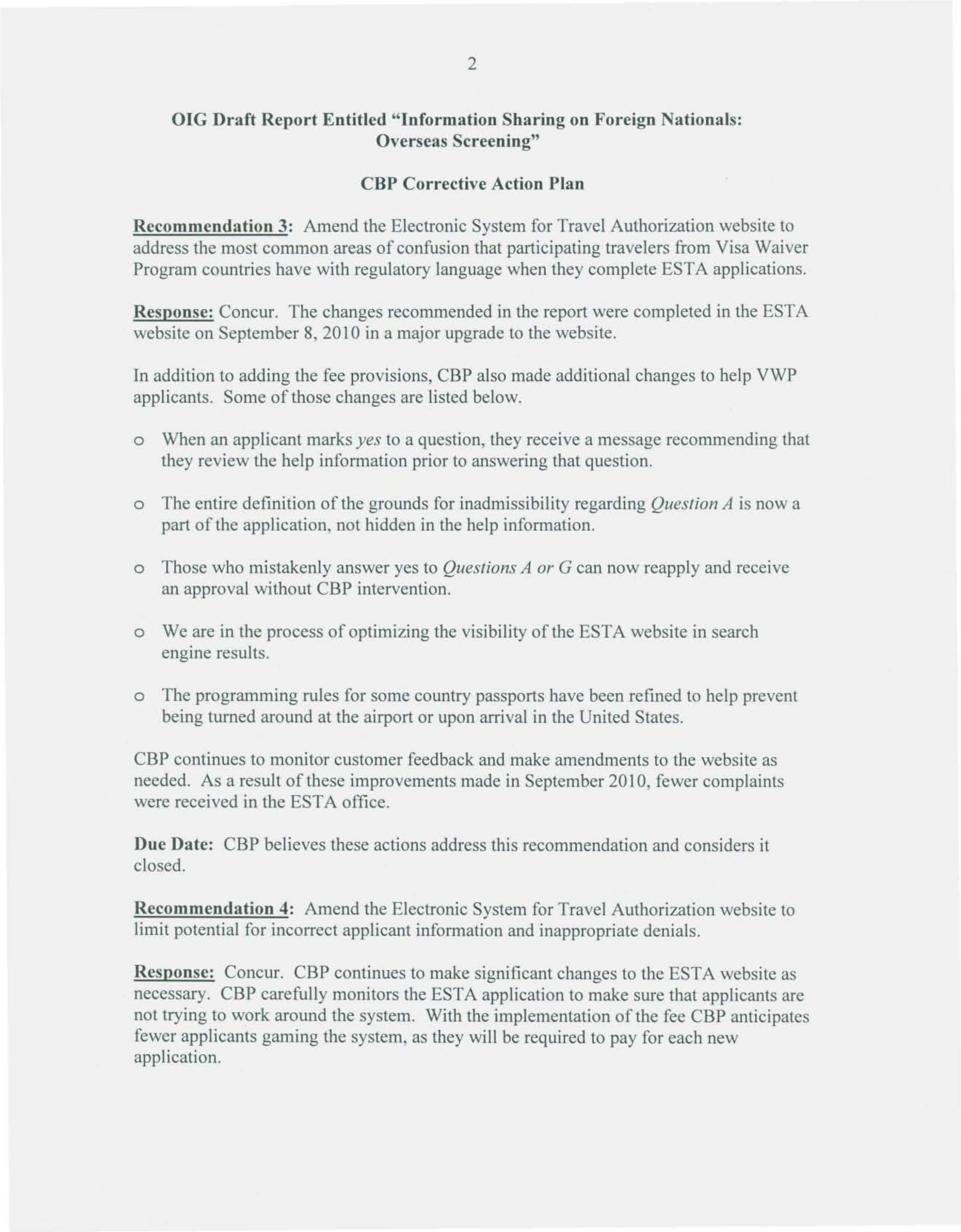
Thank you for providing us with a copy of your draft report entitled "Information Sharing on Foreign Nationals: Overseas Screening," and the opportunity to comment on the issues in this report.

Attached is U.S. Customs and Border Protection's (CBP's) formal response to the draft report that includes corrective action plans to recommendations made by OIG. CBP is concurring with eight of the nine recommendations issued and concurred in part to the remaining one recommendation involving the number of staff needed at the National Targeting Center-Passenger (NTC-P).

With regard to the classification of the draft report, CBP concurs with the Transportation Security Administration's (TSA) sensitivity comments identifying information within the report requiring restricted public access based on a designation of "For Official Use Only." CBP requests that the OIG take into consideration our concerns prior to releasing information that has been determined to be sensitive.

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Ashley Boone, CBP Audit Liaison, at (202) 344-2539.

Attachments



OIG Draft Report Entitled "Information Sharing on Foreign Nationals: Overseas Screening"

CBP Corrective Action Plan

Recommendation 3: Amend the Electronic System for Travel Authorization website to address the most common areas of confusion that participating travelers from Visa Waiver Program countries have with regulatory language when they complete ESTA applications.

Response: Concur. The changes recommended in the report were completed in the ESTA website on September 8, 2010 in a major upgrade to the website.

In addition to adding the fee provisions, CBP also made additional changes to help VWP applicants. Some of those changes are listed below.

- When an applicant marks *yes* to a question, they receive a message recommending that they review the help information prior to answering that question.

- The entire definition of the grounds for inadmissibility regarding *Question A* is now a part of the application, not hidden in the help information.

- Those who mistakenly answer yes to *Questions A or G* can now reapply and receive an approval without CBP intervention.

- We are in the process of optimizing the visibility of the ESTA website in search engine results.

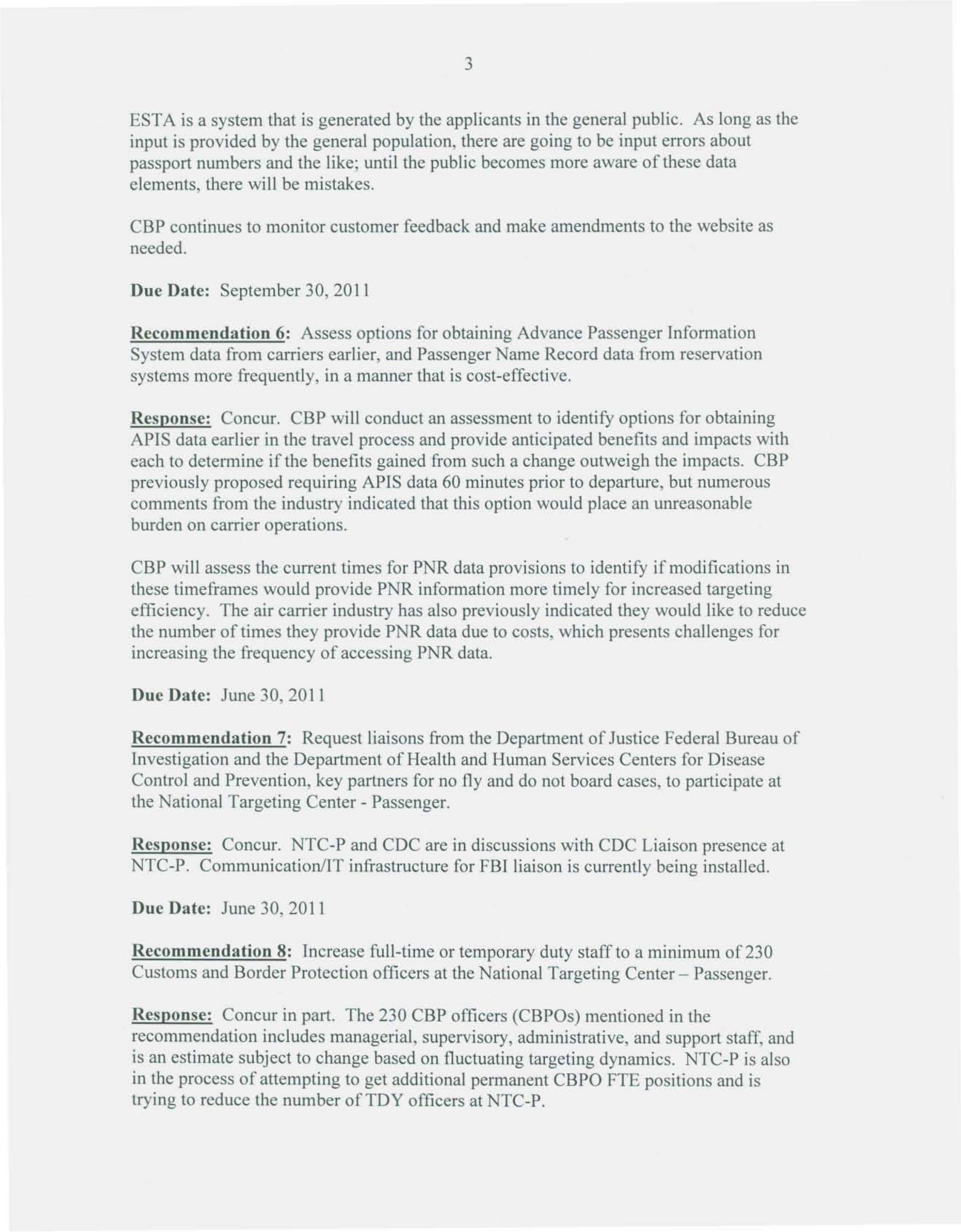
- The programming rules for some country passports have been refined to help prevent being turned around at the airport or upon arrival in the United States.

CBP continues to monitor customer feedback and make amendments to the website as needed. As a result of these improvements made in September 2010, fewer complaints were received in the ESTA office.

Due Date: CBP believes these actions address this recommendation and considers it closed.

Recommendation 4: Amend the Electronic System for Travel Authorization website to limit potential for incorrect applicant information and inappropriate denials.

Response: Concur. CBP continues to make significant changes to the ESTA website as necessary. CBP carefully monitors the ESTA application to make sure that applicants are not trying to work around the system. With the implementation of the fee CBP anticipates fewer applicants gaming the system, as they will be required to pay for each new application.



ESTA is a system that is generated by the applicants in the general public. As long as the input is provided by the general population, there are going to be input errors about passport numbers and the like; until the public becomes more aware of these data elements, there will be mistakes.

CBP continues to monitor customer feedback and make amendments to the website as needed.

Due Date: September 30, 2011

Recommendation 6: Assess options for obtaining Advance Passenger Information System data from carriers earlier, and Passenger Name Record data from reservation systems more frequently, in a manner that is cost-effective.

Response: Concur. CBP will conduct an assessment to identify options for obtaining APIS data earlier in the travel process and provide anticipated benefits and impacts with each to determine if the benefits gained from such a change outweigh the impacts. CBP previously proposed requiring APIS data 60 minutes prior to departure, but numerous comments from the industry indicated that this option would place an unreasonable burden on carrier operations.

CBP will assess the current times for PNR data provisions to identify if modifications in these timeframes would provide PNR information more timely for increased targeting efficiency. The air carrier industry has also previously indicated they would like to reduce the number of times they provide PNR data due to costs, which presents challenges for increasing the frequency of accessing PNR data.

Due Date: June 30, 2011

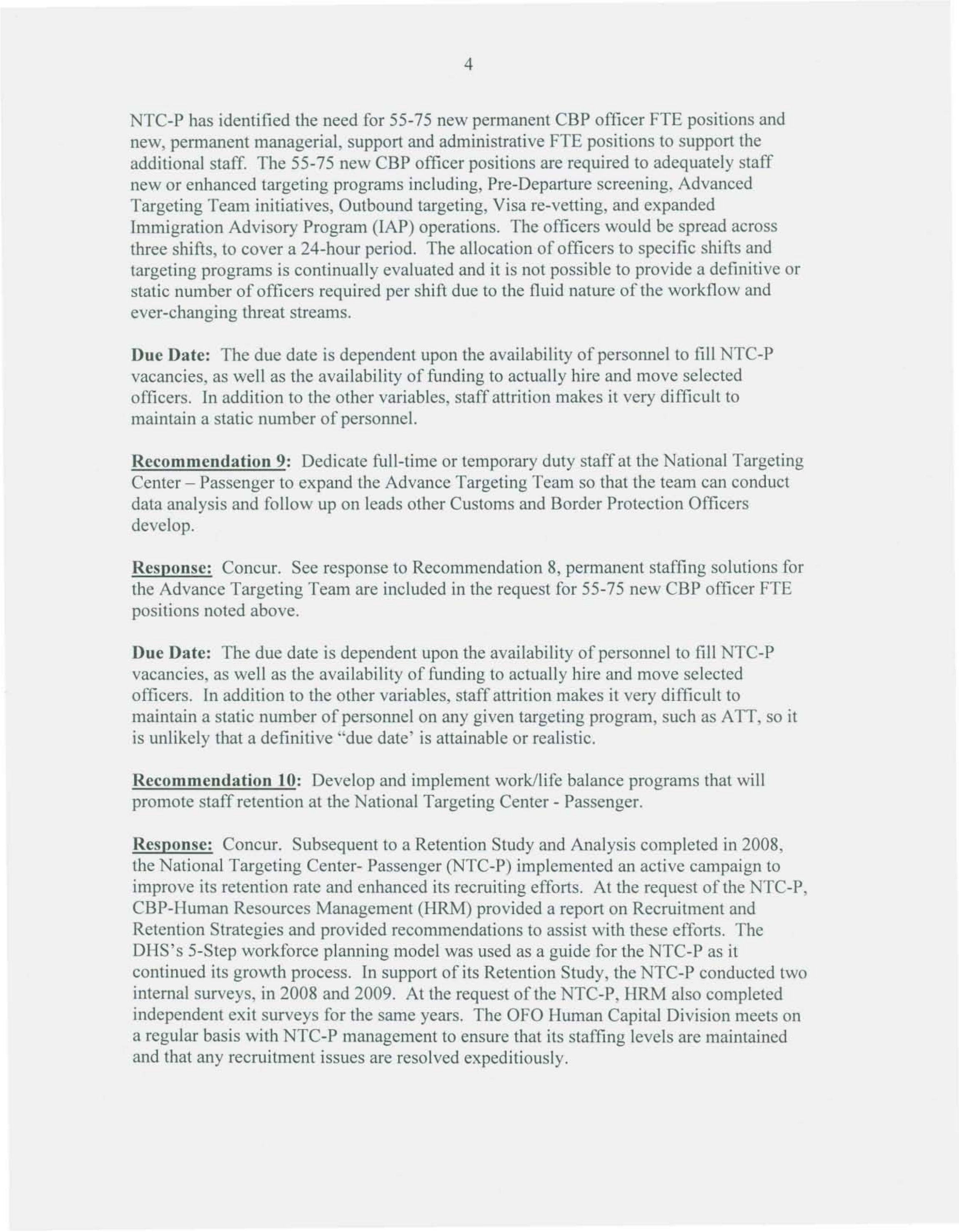
Recommendation 7: Request liaisons from the Department of Justice Federal Bureau of Investigation and the Department of Health and Human Services Centers for Disease Control and Prevention, key partners for no fly and do not board cases, to participate at the National Targeting Center - Passenger.

Response: Concur. NTC-P and CDC are in discussions with CDC Liaison presence at NTC-P. Communication/IT infrastructure for FBI liaison is currently being installed.

Due Date: June 30, 2011

Recommendation 8: Increase full-time or temporary duty staff to a minimum of 230 Customs and Border Protection officers at the National Targeting Center – Passenger.

Response: Concur in part. The 230 CBP officers (CBPOs) mentioned in the recommendation includes managerial, supervisory, administrative, and support staff, and is an estimate subject to change based on fluctuating targeting dynamics. NTC-P is also in the process of attempting to get additional permanent CBPO FTE positions and is trying to reduce the number of TDY officers at NTC-P.



NTC-P has identified the need for 55-75 new permanent CBP officer FTE positions and new, permanent managerial, support and administrative FTE positions to support the additional staff. The 55-75 new CBP officer positions are required to adequately staff new or enhanced targeting programs including, Pre-Departure screening, Advanced Targeting Team initiatives, Outbound targeting, Visa re-vetting, and expanded Immigration Advisory Program (IAP) operations. The officers would be spread across three shifts, to cover a 24-hour period. The allocation of officers to specific shifts and targeting programs is continually evaluated and it is not possible to provide a definitive or static number of officers required per shift due to the fluid nature of the workflow and ever-changing threat streams.

Due Date: The due date is dependent upon the availability of personnel to fill NTC-P vacancies, as well as the availability of funding to actually hire and move selected officers. In addition to the other variables, staff attrition makes it very difficult to maintain a static number of personnel.

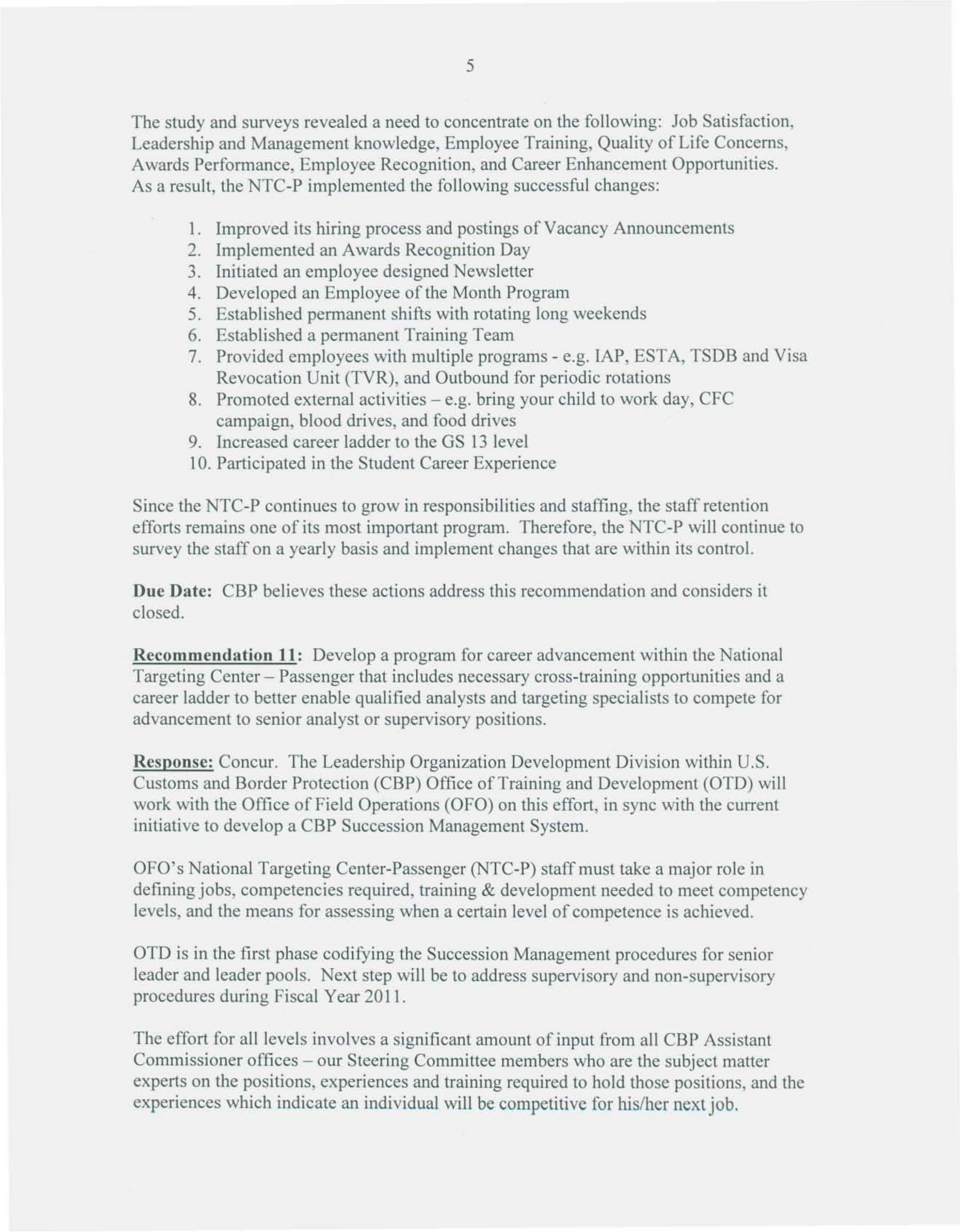
Recommendation 9: Dedicate full-time or temporary duty staff at the National Targeting Center – Passenger to expand the Advance Targeting Team so that the team can conduct data analysis and follow up on leads other Customs and Border Protection Officers develop.

Response: Concur. See response to Recommendation 8, permanent staffing solutions for the Advance Targeting Team are included in the request for 55-75 new CBP officer FTE positions noted above.

Due Date: The due date is dependent upon the availability of personnel to fill NTC-P vacancies, as well as the availability of funding to actually hire and move selected officers. In addition to the other variables, staff attrition makes it very difficult to maintain a static number of personnel on any given targeting program, such as ATT, so it is unlikely that a definitive "due date' is attainable or realistic.

Recommendation 10: Develop and implement work/life balance programs that will promote staff retention at the National Targeting Center - Passenger.

Response: Concur. Subsequent to a Retention Study and Analysis completed in 2008, the National Targeting Center- Passenger (NTC-P) implemented an active campaign to improve its retention rate and enhanced its recruiting efforts. At the request of the NTC-P, CBP-Human Resources Management (HRM) provided a report on Recruitment and Retention Strategies and provided recommendations to assist with these efforts. The DHS's 5-Step workforce planning model was used as a guide for the NTC-P as it continued its growth process. In support of its Retention Study, the NTC-P conducted two internal surveys, in 2008 and 2009. At the request of the NTC-P, HRM also completed independent exit surveys for the same years. The OFO Human Capital Division meets on a regular basis with NTC-P management to ensure that its staffing levels are maintained and that any recruitment issues are resolved expeditiously.



The study and surveys revealed a need to concentrate on the following: Job Satisfaction, Leadership and Management knowledge, Employee Training, Quality of Life Concerns, Awards Performance, Employee Recognition, and Career Enhancement Opportunities. As a result, the NTC-P implemented the following successful changes:

1. Improved its hiring process and postings of Vacancy Announcements
2. Implemented an Awards Recognition Day
3. Initiated an employee designed Newsletter
4. Developed an Employee of the Month Program
5. Established permanent shifts with rotating long weekends
6. Established a permanent Training Team
7. Provided employees with multiple programs - e.g. IAP, ESTA, TSDB and Visa Revocation Unit (TVR), and Outbound for periodic rotations
8. Promoted external activities – e.g. bring your child to work day, CFC campaign, blood drives, and food drives
9. Increased career ladder to the GS 13 level
10. Participated in the Student Career Experience

Since the NTC-P continues to grow in responsibilities and staffing, the staff retention efforts remains one of its most important program. Therefore, the NTC-P will continue to survey the staff on a yearly basis and implement changes that are within its control.

Due Date: CBP believes these actions address this recommendation and considers it closed.

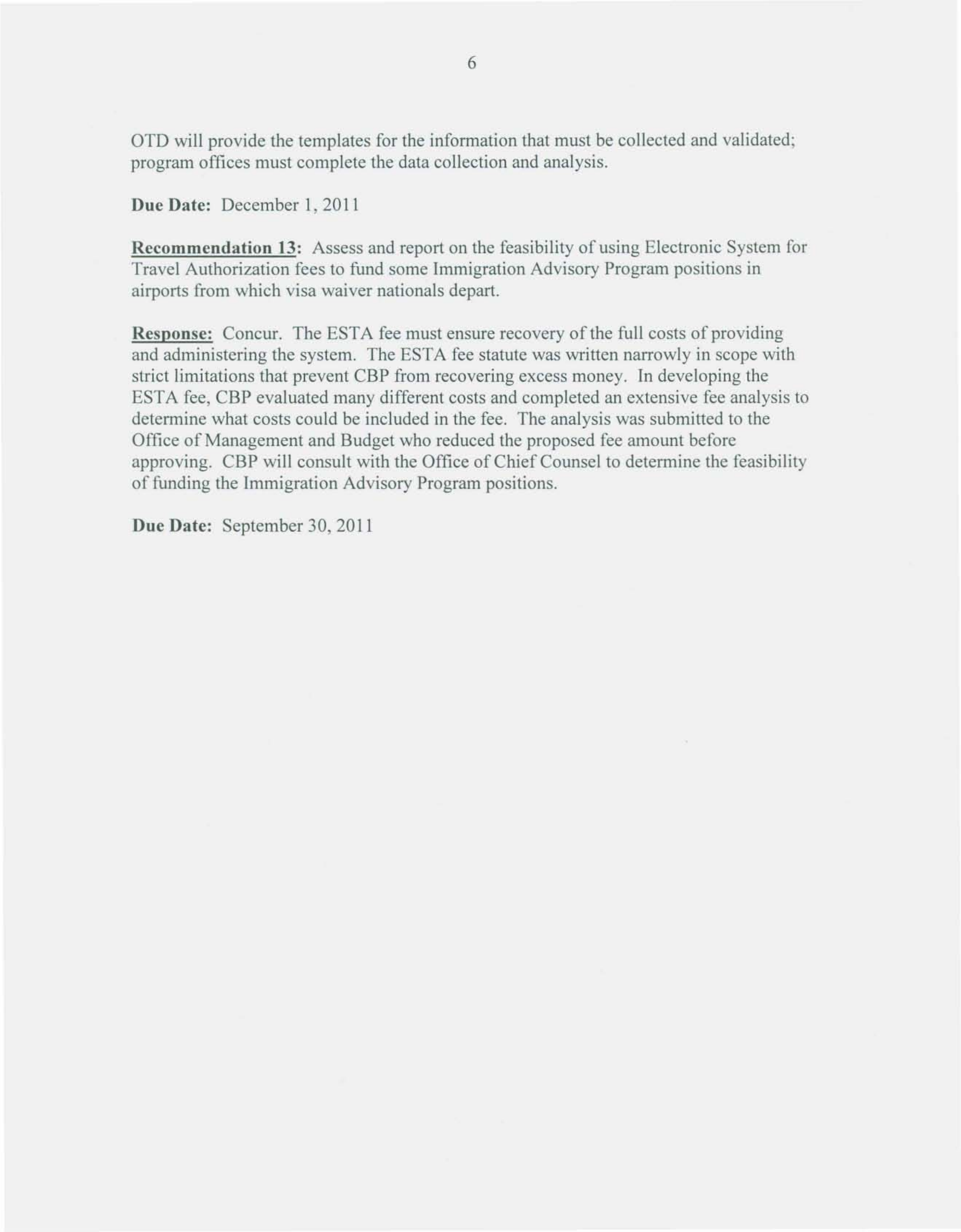
Recommendation 11: Develop a program for career advancement within the National Targeting Center – Passenger that includes necessary cross-training opportunities and a career ladder to better enable qualified analysts and targeting specialists to compete for advancement to senior analyst or supervisory positions.

Response: Concur. The Leadership Organization Development Division within U.S. Customs and Border Protection (CBP) Office of Training and Development (OTD) will work with the Office of Field Operations (OFO) on this effort, in sync with the current initiative to develop a CBP Succession Management System.

OFO's National Targeting Center-Passenger (NTC-P) staff must take a major role in defining jobs, competencies required, training & development needed to meet competency levels, and the means for assessing when a certain level of competence is achieved.

OTD is in the first phase codifying the Succession Management procedures for senior leader and leader pools. Next step will be to address supervisory and non-supervisory procedures during Fiscal Year 2011.

The effort for all levels involves a significant amount of input from all CBP Assistant Commissioner offices – our Steering Committee members who are the subject matter experts on the positions, experiences and training required to hold those positions, and the experiences which indicate an individual will be competitive for his/her next job.



OTD will provide the templates for the information that must be collected and validated; program offices must complete the data collection and analysis.

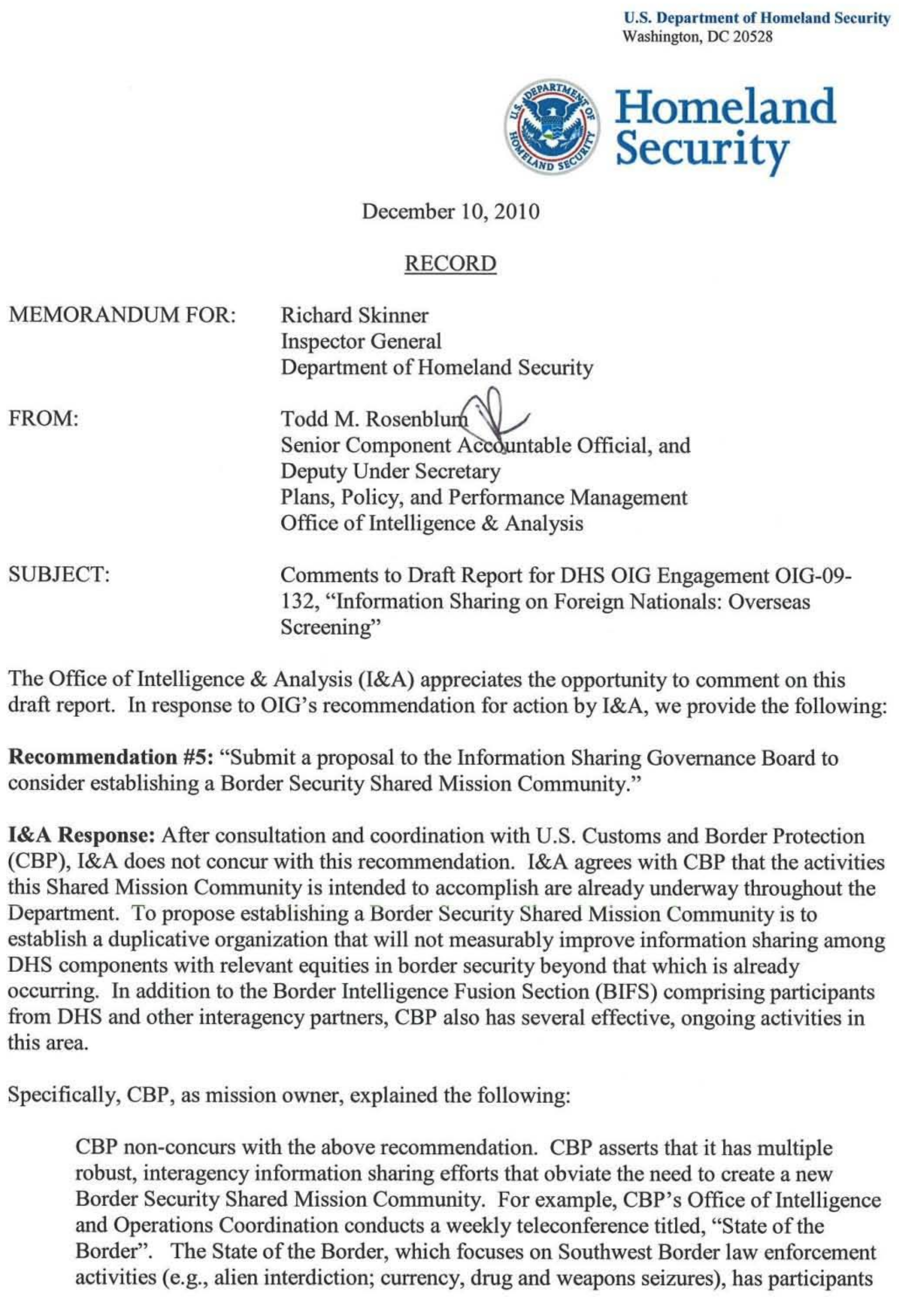
Due Date: December 1, 2011

Recommendation 13: Assess and report on the feasibility of using Electronic System for Travel Authorization fees to fund some Immigration Advisory Program positions in airports from which visa waiver nationals depart.

Response: Concur. The ESTA fee must ensure recovery of the full costs of providing and administering the system. The ESTA fee statute was written narrowly in scope with strict limitations that prevent CBP from recovering excess money. In developing the ESTA fee, CBP evaluated many different costs and completed an extensive fee analysis to determine what costs could be included in the fee. The analysis was submitted to the Office of Management and Budget who reduced the proposed fee amount before approving. CBP will consult with the Office of Chief Counsel to determine the feasibility of funding the Immigration Advisory Program positions.

Due Date: September 30, 2011

Appendix B
Management Comments to the Draft Report



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

Homeland
Security

December 10, 2010

RECORD

MEMORANDUM FOR: Richard Skinner
Inspector General
Department of Homeland Security

FROM: Todd M. Rosenblum
Senior Component Accountable Official, and
Deputy Under Secretary
Plans, Policy, and Performance Management
Office of Intelligence & Analysis

SUBJECT: Comments to Draft Report for DHS OIG Engagement OIG-09-132, "Information Sharing on Foreign Nationals: Overseas Screening"

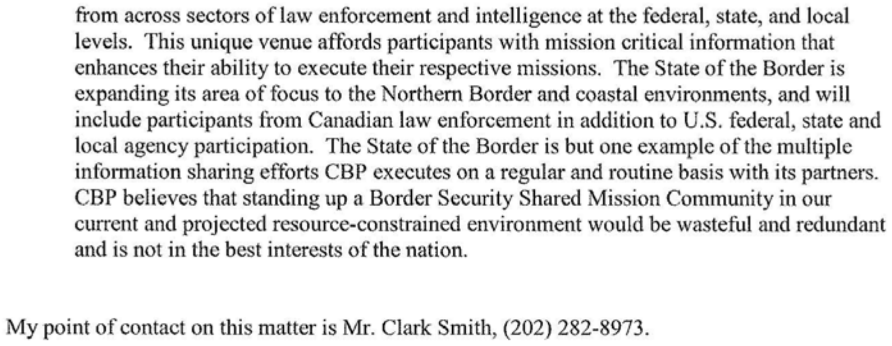
The Office of Intelligence & Analysis (I&A) appreciates the opportunity to comment on this draft report. In response to OIG's recommendation for action by I&A, we provide the following:

Recommendation #5: "Submit a proposal to the Information Sharing Governance Board to consider establishing a Border Security Shared Mission Community."

I&A Response: After consultation and coordination with U.S. Customs and Border Protection (CBP), I&A does not concur with this recommendation. I&A agrees with CBP that the activities this Shared Mission Community is intended to accomplish are already underway throughout the Department. To propose establishing a Border Security Shared Mission Community is to establish a duplicative organization that will not measurably improve information sharing among DHS components with relevant equities in border security beyond that which is already occurring. In addition to the Border Intelligence Fusion Section (BIFS) comprising participants from DHS and other interagency partners, CBP also has several effective, ongoing activities in this area.

Specifically, CBP, as mission owner, explained the following:

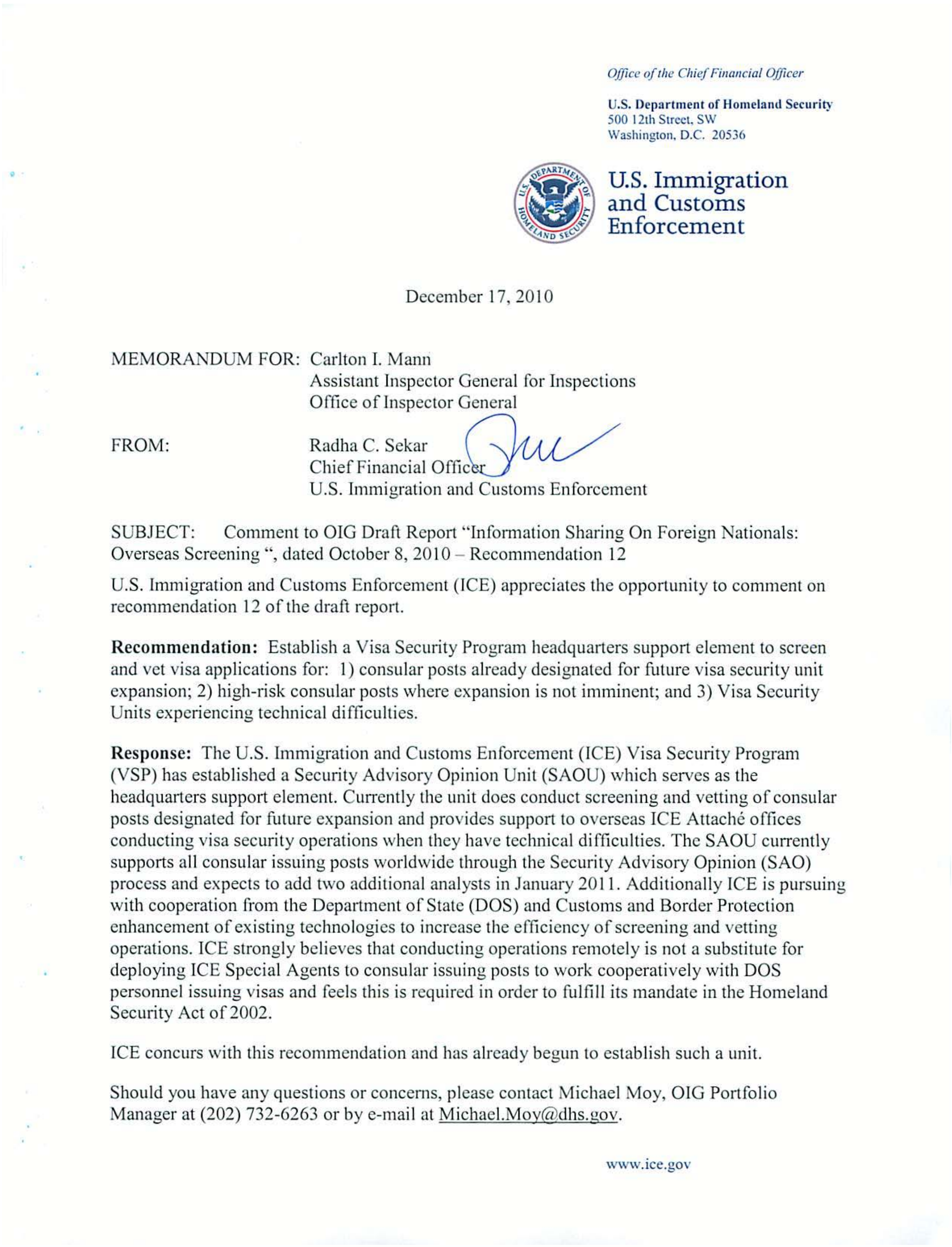
> CBP non-concurs with the above recommendation. CBP asserts that it has multiple robust, interagency information sharing efforts that obviate the need to create a new Border Security Shared Mission Community. For example, CBP's Office of Intelligence and Operations Coordination conducts a weekly teleconference titled, "State of the Border". The State of the Border, which focuses on Southwest Border law enforcement activities (e.g., alien interdiction; currency, drug and weapons seizures), has participants



from across sectors of law enforcement and intelligence at the federal, state, and local levels. This unique venue affords participants with mission critical information that enhances their ability to execute their respective missions. The State of the Border is expanding its area of focus to the Northern Border and coastal environments, and will include participants from Canadian law enforcement in addition to U.S. federal, state and local agency participation. The State of the Border is but one example of the multiple information sharing efforts CBP executes on a regular and routine basis with its partners. CBP believes that standing up a Border Security Shared Mission Community in our current and projected resource-constrained environment would be wasteful and redundant and is not in the best interests of the nation.

My point of contact on this matter is Mr. Clark Smith, (202) 282-8973.

Appendix B
Management Comments to the Draft Report



Office of the Chief Financial Officer

U.S. Department of Homeland Security
500 12th Street, SW
Washington, D.C. 20536

U.S. Immigration
and Customs
Enforcement

December 17, 2010

MEMORANDUM FOR: Carlton I. Mann
Assistant Inspector General for Inspections
Office of Inspector General

FROM: Radha C. Sekar
Chief Financial Officer
U.S. Immigration and Customs Enforcement

SUBJECT: Comment to OIG Draft Report "Information Sharing On Foreign Nationals: Overseas Screening ", dated October 8, 2010 – Recommendation 12

U.S. Immigration and Customs Enforcement (ICE) appreciates the opportunity to comment on recommendation 12 of the draft report.

Recommendation: Establish a Visa Security Program headquarters support element to screen and vet visa applications for: 1) consular posts already designated for future visa security unit expansion; 2) high-risk consular posts where expansion is not imminent; and 3) Visa Security Units experiencing technical difficulties.

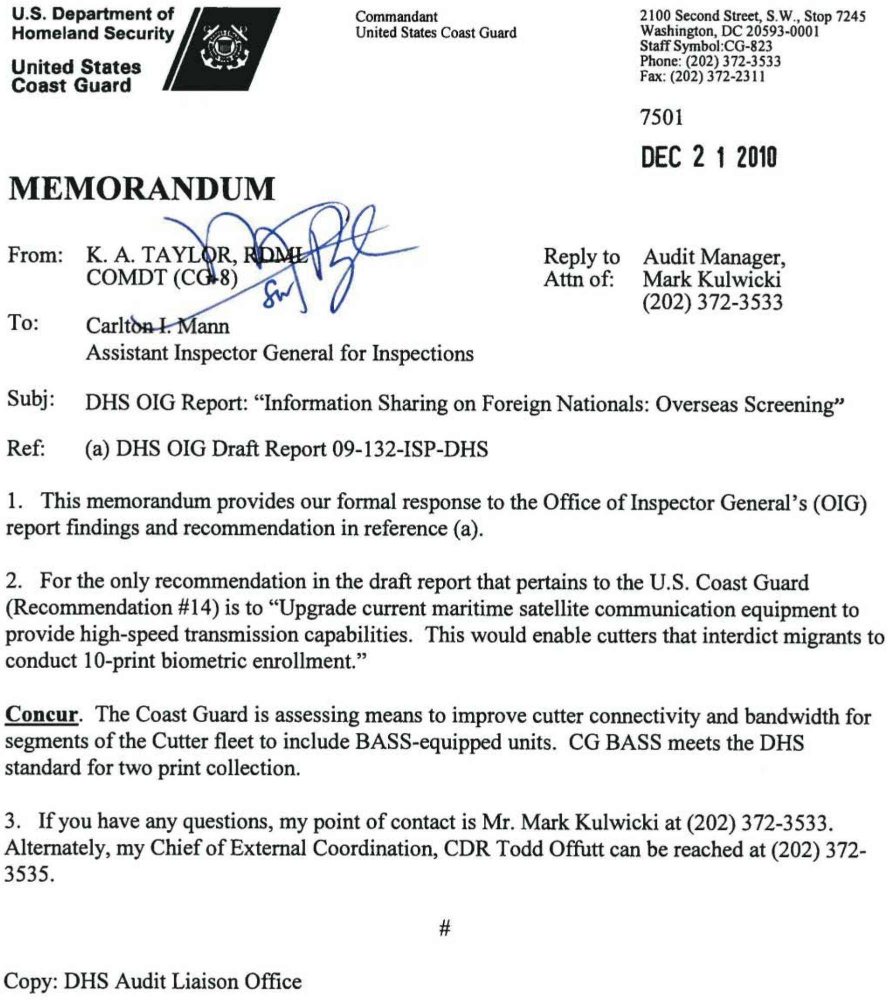
Response: The U.S. Immigration and Customs Enforcement (ICE) Visa Security Program (VSP) has established a Security Advisory Opinion Unit (SAOU) which serves as the headquarters support element. Currently the unit does conduct screening and vetting of consular posts designated for future expansion and provides support to overseas ICE Attaché offices conducting visa security operations when they have technical difficulties. The SAOU currently supports all consular issuing posts worldwide through the Security Advisory Opinion (SAO) process and expects to add two additional analysts in January 2011. Additionally ICE is pursuing with cooperation from the Department of State (DOS) and Customs and Border Protection enhancement of existing technologies to increase the efficiency of screening and vetting operations. ICE strongly believes that conducting operations remotely is not a substitute for deploying ICE Special Agents to consular issuing posts to work cooperatively with DOS personnel issuing visas and feels this is required in order to fulfill its mandate in the Homeland Security Act of 2002.

ICE concurs with this recommendation and has already begun to establish such a unit.

Should you have any questions or concerns, please contact Michael Moy, OIG Portfolio Manager at (202) 732-6263 or by e-mail at Michael.Moy@dhs.gov.

www.ice.gov

Appendix B
Management Comments to the Draft Report



U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W., Stop 7245
Washington, DC 20593-0001
Staff Symbol:CG-823
Phone: (202) 372-3533
Fax: (202) 372-2311

7501

DEC 2 1 2010

MEMORANDUM

From: K. A. TAYLOR, RDML
COMDT (CG-8)

Reply to Attn of: Audit Manager,
Mark Kulwicki
(202) 372-3533

To: Carlton I. Mann
Assistant Inspector General for Inspections

Subj: DHS OIG Report: "Information Sharing on Foreign Nationals: Overseas Screening"

Ref: (a) DHS OIG Draft Report 09-132-ISP-DHS

1. This memorandum provides our formal response to the Office of Inspector General's (OIG) report findings and recommendation in reference (a).

2. For the only recommendation in the draft report that pertains to the U.S. Coast Guard (Recommendation #14) is to "Upgrade current maritime satellite communication equipment to provide high-speed transmission capabilities. This would enable cutters that interdict migrants to conduct 10-print biometric enrollment."

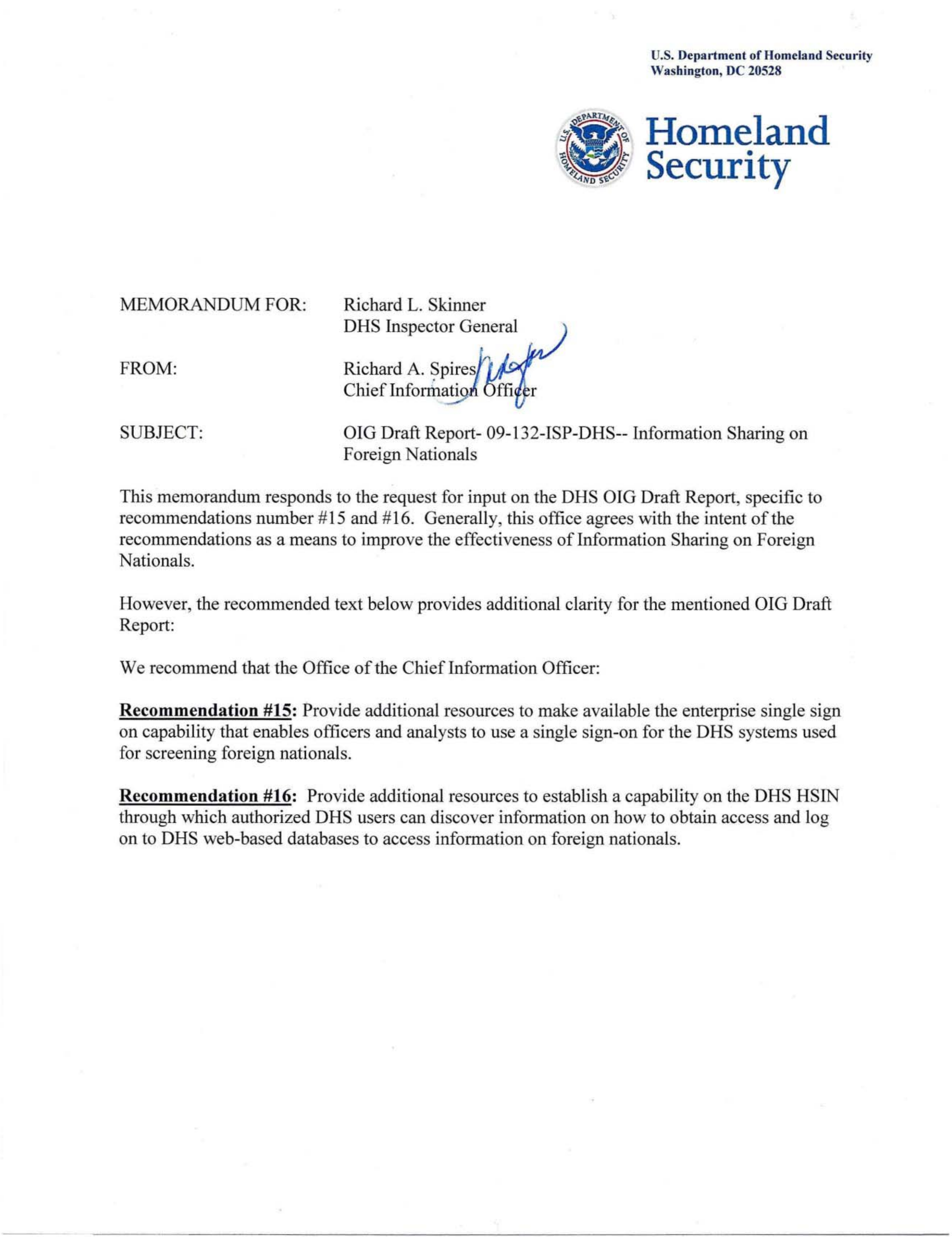
Concur. The Coast Guard is assessing means to improve cutter connectivity and bandwidth for segments of the Cutter fleet to include BASS-equipped units. CG BASS meets the DHS standard for two print collection.

3. If you have any questions, my point of contact is Mr. Mark Kulwicki at (202) 372-3533. Alternately, my Chief of External Coordination, CDR Todd Offutt can be reached at (202) 372-3535.

#

Copy: DHS Audit Liaison Office

Appendix B
Management Comments to the Draft Report



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

Homeland
Security

MEMORANDUM FOR: Richard L. Skinner
DHS Inspector General

FROM: Richard A. Spires
Chief Information Officer

SUBJECT: OIG Draft Report- 09-132-ISP-DHS-- Information Sharing on Foreign Nationals

This memorandum responds to the request for input on the DHS OIG Draft Report, specific to recommendations number #15 and #16. Generally, this office agrees with the intent of the recommendations as a means to improve the effectiveness of Information Sharing on Foreign Nationals.

However, the recommended text below provides additional clarity for the mentioned OIG Draft Report:

We recommend that the Office of the Chief Information Officer:

Recommendation #15: Provide additional resources to make available the enterprise single sign on capability that enables officers and analysts to use a single sign-on for the DHS systems used for screening foreign nationals.

Recommendation #16: Provide additional resources to establish a capability on the DHS HSIN through which authorized DHS users can discover information on how to obtain access and log on to DHS web-based databases to access information on foreign nationals.

Appendix C
Authorities for Information Sharing on Foreign Nationals

Authorities for Information Sharing on Foreign Nationals

Statutory Authority

Immigration and Nationality Act (as amended)

- Specifies which foreign nationals are eligible to be admitted lawfully into the United States, which are not eligible for security, safety, public interest, and public health reasons, and which can apply to receive a waiver that allows them to be admitted. (Section 212).[34]

Aviation and Transportation Security Act of 2001 (PL 107-71)

- Provides mandatory manifest and passenger name record requirements, among other aviation screening requirements. (Section 115).[35]

Enhanced Border Security and Visa Entry Reform Act of 2002 (PL 107-173)

- Requires enhancements to visa issuance technologies (Title III, Section 303)
  - Requires DHS and the Department of State to issue aliens only biometric-based, machine-readable, tamper-resistant visas and other travel and entry documents.
  - Requires DHS to provide equipment and software to allow biometric comparison and authentication at ports of entry.[36]
  - Requires visa waiver governments to use machine-readable, tamper-resistant passports that incorporate biometric and document authentication.[37]
- Requires DHS to track foreign student or exchange visitor program participants (Title V, Section 501).
- Updates requirements for electronic transmission of passenger and crew manifests for flights and vessels that arrive or depart from the United States (Title 4, Section 402).[38]

Homeland Security Act of 2002 (PL 107-296)

- Requires, unless otherwise directed by the President, that the DHS Secretary shall have access to all information that relates to threats of terrorism against the United States that may be collected, possessed, or prepared by any agency of the federal government (Title II, Section 202).
- Creates DHS, authorizes the DHS Secretary to administer and enforce the Immigration and Nationality Act and other laws that relate to visas; refuse visas for individual applicants; assign DHS officers to diplomatic posts to perform visa security activities; initiate investigations of visa security-related matters; and provide advice and training to consular officers (Title IV, Section 428)[39]
- Establishes procedures to share federal government information with DHS (Title VIII, Section 892).

[34] 8 U.S.C. Section 1182.

[35] 49 U.S.C. Section 114.

[36] 8 U.S.C. Section 1365b.

[37] 8 U.S.C. Section 1187.

[38] 8 U.S.C. Section 1221.

[39] 6 U.S.C. Section 236.

Appendix C
Authorities for Information Sharing on Foreign Nationals

Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458)

- Requires guidelines for information sharing and establishes a federal Information Sharing Council to identify gaps in technologies, programs, and systems used by the federal government to share information (Title I, Section 1016)
- Requires in-person interviews for most visas (Title V, Section 5301)[40]
- Requires the Department of State to appoint an anti-fraud specialist to each high-fraud consular office that does not have a DHS visa security unit (Title VII, Section 7203)
- Calls for international sharing of information on lost and stolen passports and other travel documents (Title VII, Section 7204)
- Calls for the Immigration Advisory Programs to be established in at least 50 foreign airports (Title VII, Section 7206)[41]
- Requires integration of all databases and data systems that process or contain information on aliens that are maintained by DHS ICE, CBP, and USCIS, Department of State Consular Affairs, and Department of Justice Executive Office for Immigration Review (Title VII, Section 7208)[42]
- Requires DHS to assume from aircraft operators the function of preflight comparisons of airline passenger information to federal government watch lists for domestic flights and international flights to, from, and over the United States (Secure Flight) (Title IV, Section 4012(a))[43]

Implementing Recommendations of the 9/11 Commission Act of 2007 (PL 110-53)

- Requires Visa Waiver Program governments to share information on whether their citizens represent a threat to the United States, and information on lost and stolen passports (Title VII, Section 711)[44]
- Requires Visa Waiver Program nationals to obtain an ESTA approval before they travel (Title VII, Section 711)
- Provides DHS authority to admit into the Visa Waiver Program countries that otherwise meet requirements, but have refusal rates up to 10% (the prior threshold was 3%), provided countries meet certain conditions for security and information sharing (Title VII, Section 711).
- Requires DHS to ensure effective coordination, with respect to policies, programs, plans, operations, and dissemination of intelligence and information related to terrorist travel, among DHS operational components and with other federal agencies (Title VII, Section 722)[45]

[40] 8 U.S.C. Section 1202.

[41] 8 U.S.C. Section 1225a (b).

[42] 8 U.S.C. Section 1365b.

[43] 49 U.S.C. Section 44903(j)(2).

[44] 8 U.S.C. Section 1187.

[45] 6 U.S.C. Section 123.

Appendix C
Authorities for Information Sharing on Foreign Nationals

Executive Authority
Homeland Security Presidential Directive 6, September 16, 2003
➢ Establishes policy to develop, integrate and maintain thorough, accurate, and current information about individuals known or suspected to be engaged in terrorism.[46]
Executive Order 13388, October 25, 2005
➢ Requires federal agencies to give high priority to detecting and preventing terrorist activities, and to the interchange of terrorism information.[47]
DHS Secretary Memorandum, DHS Policy for Internal Information Exchange and Sharing, February 1, 2007 ("One DHS" Memorandum)
➢ Requires each DHS component to give the highest priority to the sharing of potential terrorism, homeland security, law enforcement, and related information.[48]
White House Memorandum, Strengthening Information Sharing and Access, July 2, 2009
➢ States, "Achieving effective information sharing and access throughout the government is a top priority of the Obama administration. This priority extends beyond terrorism-related issues, to the sharing of information more broadly to enhance the national security of the United States and the safety of the American people."[49]

[46] http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm

[47] http://edocket.access.gpo.gov/2005/pdf/05-21571.pdf

[48] Memorandum from DHS Secretary Michael A. Chertoff to All Department of Homeland Security Components, *DHS Policy for Internal Information Exchange and Sharing*, February 1, 2007.

[49] Memorandum from John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, to cabinet level officials, *Strengthening Information Sharing And Access*, July 2, 2009.

Appendix D
Visa Waiver Program Countries

Visa Waiver Program Countries

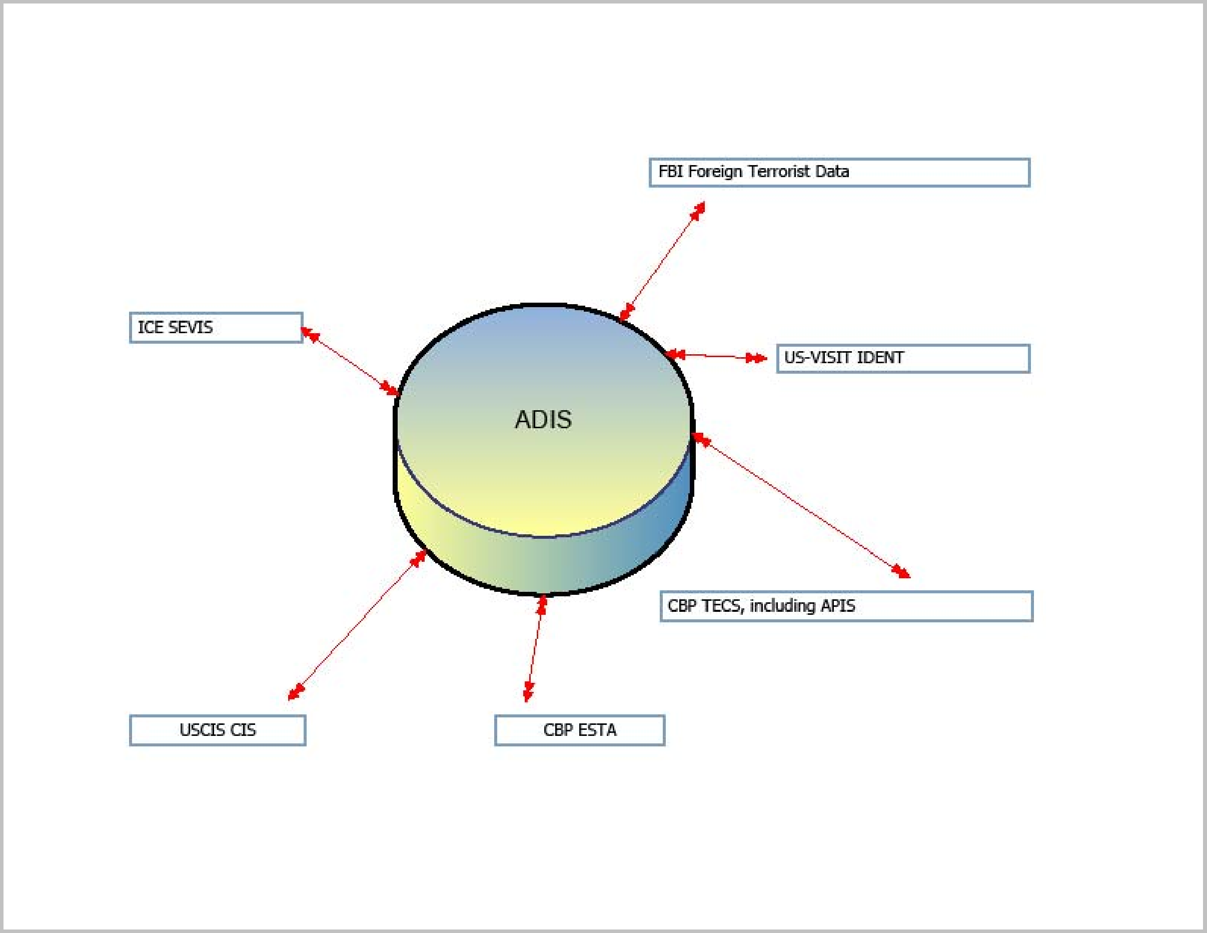
As Of May 2010

- Andorra
- Australia
- Austria
- Belgium
- Brunei
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Japan
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Monaco
- The Netherlands
- New Zealand
- Norway
- Portugal
- San Marino
- Singapore
- Slovakia
- Slovenia
- South Korea
- Spain
- Sweden
- Switzerland
- United Kingdom

Definitions and Diagram of DHS Systems

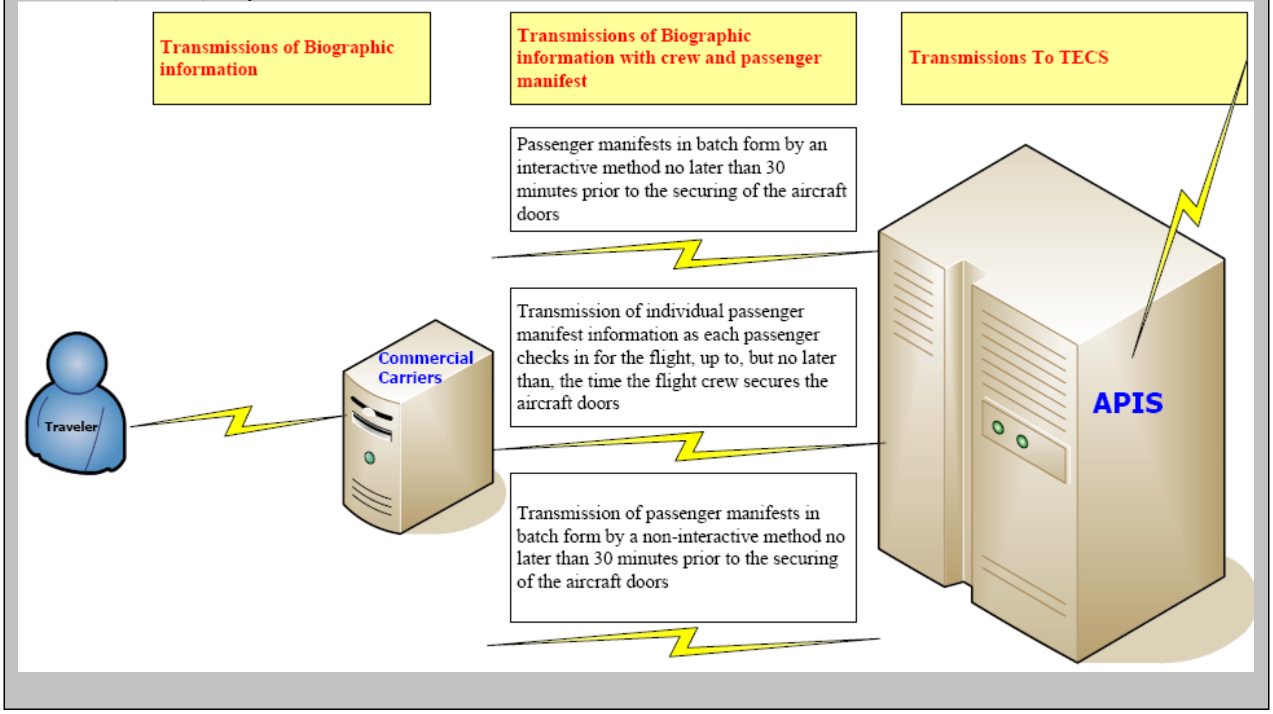
Arrival and Departure Information System (ADIS) *(Owner US-VISIT*)

The Arrival and Departure Information System (ADIS) is used to collect, match, and report in US-VISIT on international arrivals and departures of many categories of non-U.S. citizens.



Advance Passenger Information System (APIS) *(Owner CBP)*

The Advance Passenger Information System (APIS) is a widely used electronic data interchange system that allows air carriers to transmit traveler data to CBP.[50] Complete APIS data for each passenger are required no later than 30 minutes before the aircraft is secured for airlines that provide a list of passenger names and no later than when the aircraft is secured for electronic APIS Quick Query submissions.[51] APIS information is maintained as a module within TECS.


Transmissions of Biographic information
Transmissions of Biographic information with crew and passenger manifest
Transmissions To TECS
Traveler
Commercial Carriers
APIS

Passenger manifests in batch form by an interactive method no later than 30 minutes prior to the securing of the aircraft doors

Transmission of individual passenger manifest information as each passenger checks in for the flight, up to, but no later than, the time the flight crew secures the aircraft doors

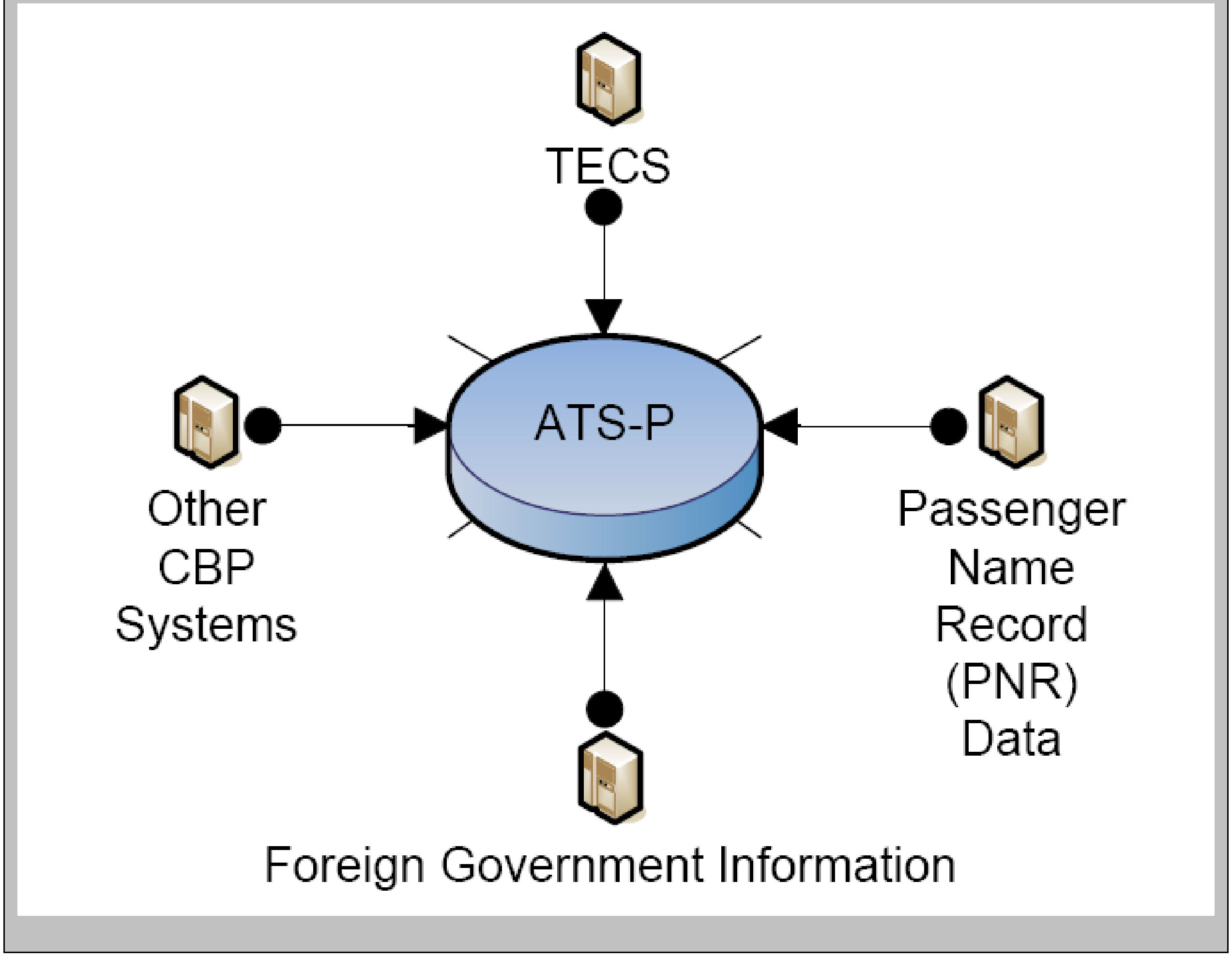
Transmission of passenger manifests in batch form by a non-interactive method no later than 30 minutes prior to the securing of the aircraft doors

[50] http://www.cbp.gov/linkhandler/cgov/travel/inspections_carriers_facilities/apis/apis_factsheet.ctt/apis_factsheet.pdf

[51] http://www.cbp.gov/linkhandler/cgov/travel/inspections_carriers_facilities/apis/apis_faqs.ctt/apis_faqs.doc

Automated Targeting System - Passenger (ATS-P) *(Owner CBP)*

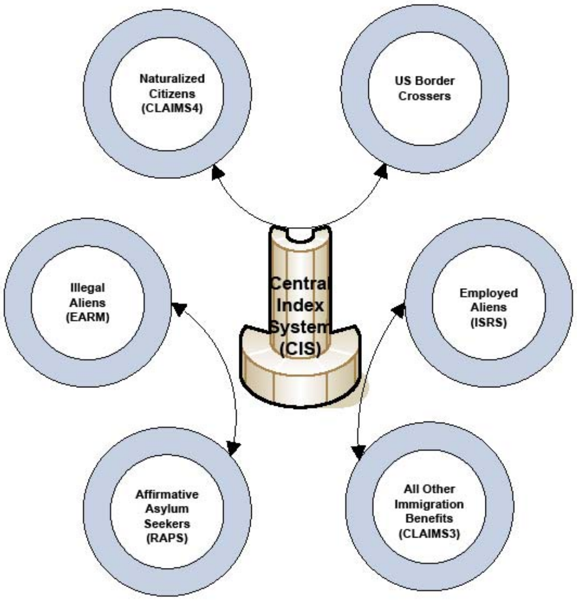
Automated Targeting System – Passenger (ATS-P) is a web-based enforcement and decision support tool used to collect, analyze, and disseminate information. ATS-P receives various data from CBP systems, which includes TECS, Passenger Name Records (PNR) from airlines, and lookout information from foreign governments.


TECS
ATS-P
Other CBP Systems
Passenger Name Record (PNR) Data
Foreign Government Information

Central Index System (CIS) *(Owner USCIS)*

The Central Index System (CIS) contains information on the status of 57 million applicant and petitioners who seek immigration benefits, denied and approved refugee determinations, as well as the status of other individuals subject to the provisions of the Immigration and Nationality Act, to include:[52]

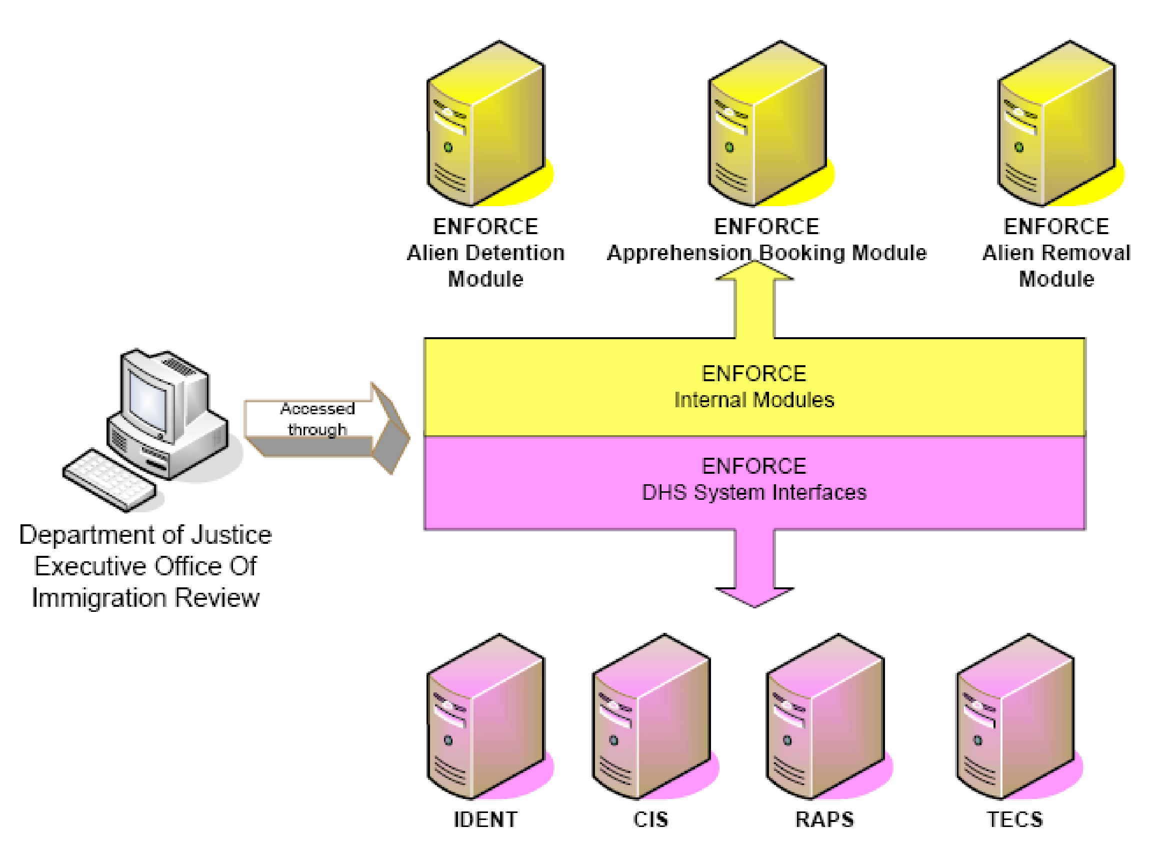
- Naturalized citizens
  - Computer-Linked Application Information Management System 4 (CLAIMS4)
- Individuals who apply for affirmative asylum status, and certain applications for benefits under the Nicaraguan Adjustment and Central American Relief Act
  - Refugees Asylum and Parole System (RAPS)
- United States border crossers
  - Alien Registration Card / Border Crossing Card Interface
- All USCIS immigration benefits other than naturalization and humanitarian immigration benefits
  - Computer-Linked Application Information Management System 3 (CLAIMS3)
- Aliens who illegally entered the United States
  - ENFORCE Alien Removal Module (EARM)
- Aliens who have been issued employment authorization documents
  - Image Storage and Retrieval System (ISRS)


Naturalized Citizens (CLAIMS4)
US Border Crossers
Illegal Aliens (EARM)
Central Index System (CIS)
Employed Aliens (ISRS)
Affirmative Asylum Seekers (RAPS)
All Other Immigration Benefits (CLAIMS3)

[52] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_cis.pdf

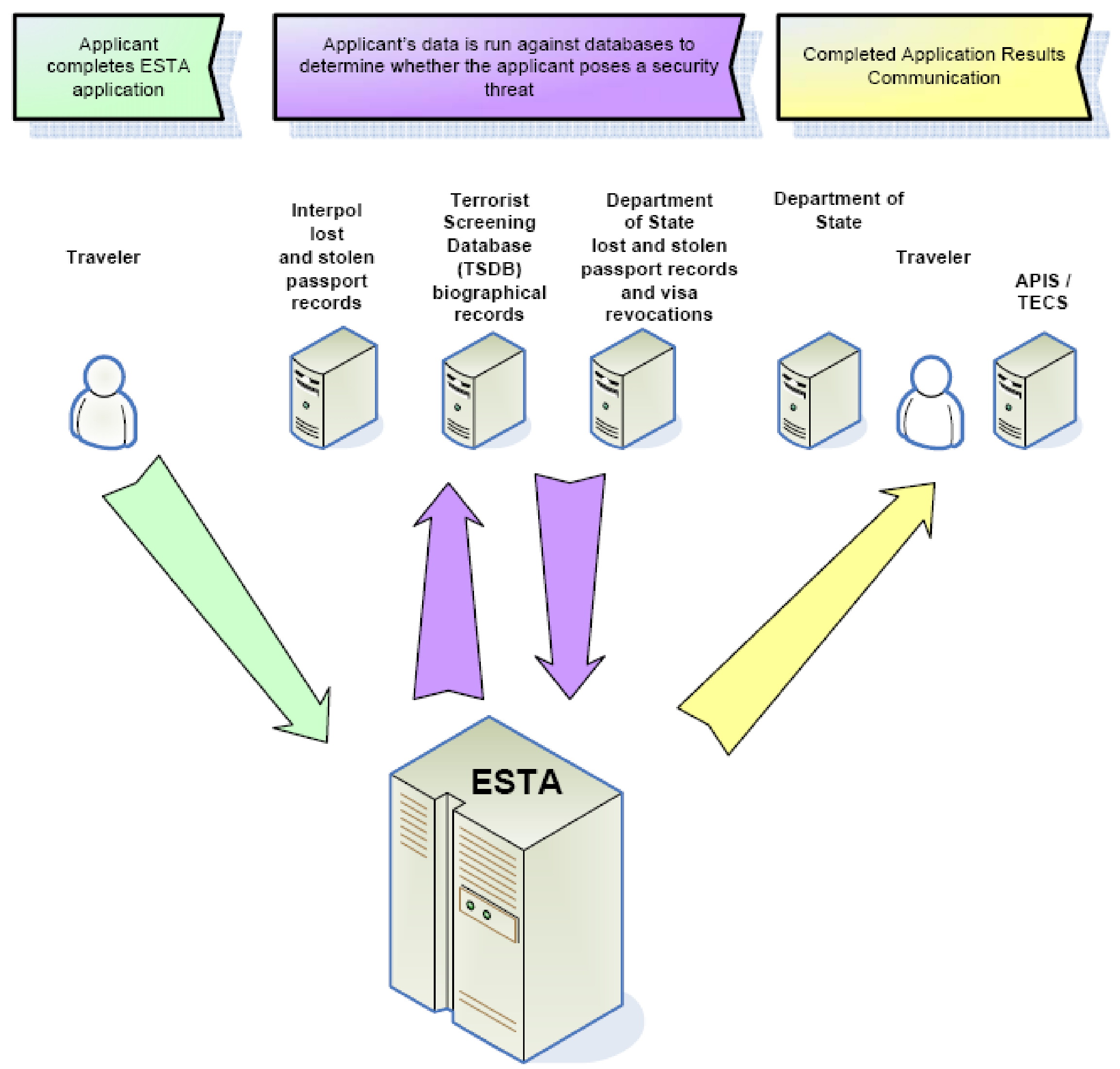
ENFORCE / Enforce Alien Removal Module (EARM) *(Owner ICE)*

- Immigration Enforcement Operational Records System (ENFORCE) contains modules to manage ICE and CBP law enforcement functions:
  - *ENFORCE Apprehension Booking Module* tracks apprehension of individuals ICE and CBP arrested for violations of customs and immigration laws.
  - *ENFORCE Alien Detention Module* tracks the detention of subjects in ICE custody charged with violations of the Immigration and Nationality Act.
  - *ENFORCE Alien Removal Module (EARM)* is used to document the processing and removal of aliens, track the status of alien removal proceedings, and provide information on an alien's entire detention history.
- ENFORCE interfaces with TECS, IDENT, USCIS, Refugees, Asylum, and Parole System (RAPS), and other DHS systems.
- ENFORCE also interfaces with the Department of Justice Executive Office of Immigration Review database used to place aliens in removal proceedings and track their case dispositions.



Electronic System for Travel Authorization (ESTA) *(Owner CBP)*

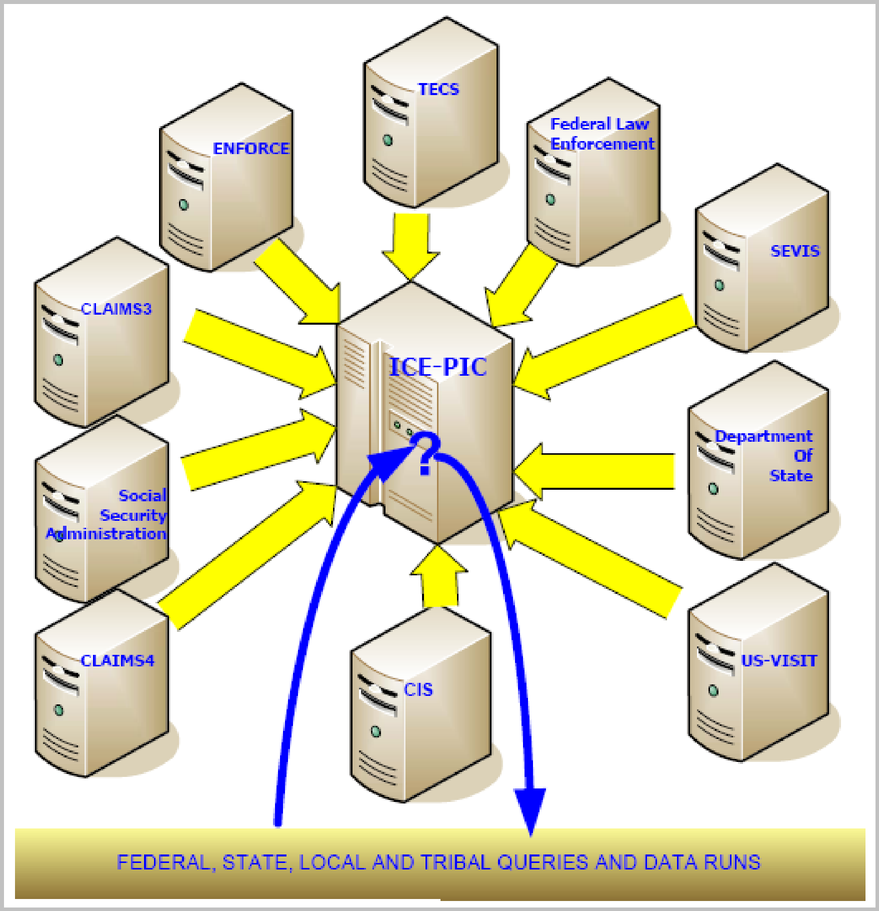
Electronic System for Travel Authorization (ESTA) is a fully automated electronic travel authorization system that determines the eligibility of visitors to travel to the United States under the Visa Waiver Program and whether such travel poses a law enforcement or security risk. Upon receipt of an ESTA application, CBP examines the application and screen applicant data through law enforcement systems.[53]


Applicant completes ESTA application
Applicant's data is run against databases to determine whether the applicant poses a security threat
Completed Application Results Communication
Traveler
Interpol lost and stolen passport records
Terrorist Screening Database (TSDB) biographical records
Department of State lost and stolen passport records and visa revocations
Department of State
Traveler
APIS / TECS
ESTA

[53] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_esta.pdf

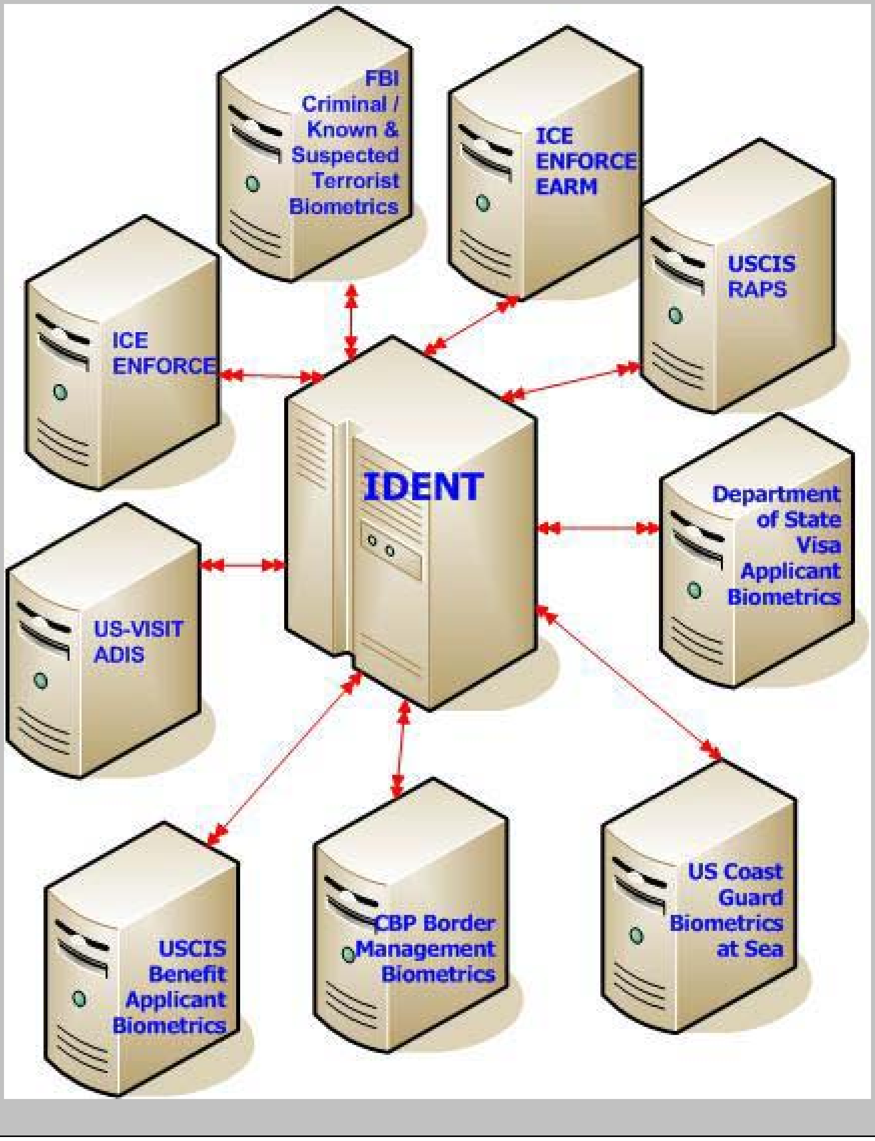
ICE-PIC *(Owner ICE)*

Immigration and Customs Enforcement (ICE) Pattern Analysis and Information Collection System (ICE-PIC) enables pattern and data analysis to find previously unknown relationship data.[54] The database program compiles information on immigrants and other individuals. ICE-PIC receives information, but does not send information back to these systems. Federal, state, local, and tribal law enforcement may use the information aggregated in ICE-PIC for queries, data runs, and data analysis.[55]



[54] http://www.ice.gov/pi/news/factsheets/icepic htm
[55] http://www.dhs.gov/xlibrary/assets/privacy/privacy_data_%20mining_%20report.pdf/

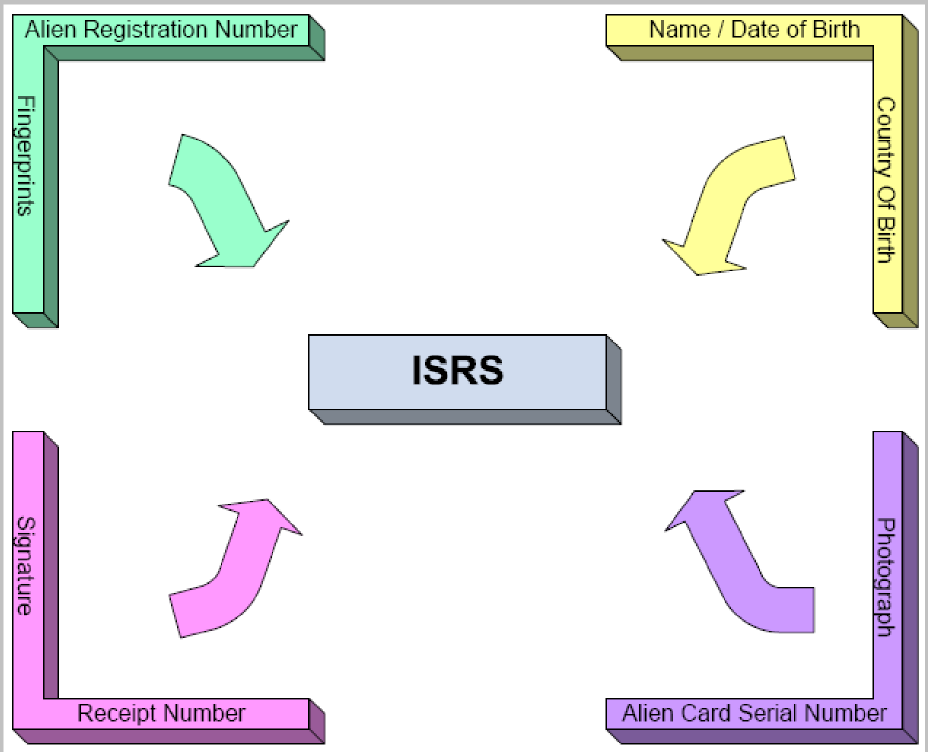
IDENT ***(Owner US-VISIT)***
Automated Biometric Identification System (IDENT) is a DHS-wide system to collect and process biometric and limited biographic information for DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.[56] IDENT has an automated interface with biometrics in the FBI's biometric system. Other federal agencies can check biometrics against IDENT, but are not automated to send or receive updated status information.


FBI Criminal / Known & Suspected Terrorist Biometrics
ICE ENFORCE EARM
USCIS RAPS
ICE ENFORCE
IDENT
Department of State Visa Applicant Biometrics
US-VISIT ADIS
USCIS Benefit Applicant Biometrics
CBP Border Management Biometrics
US Coast Guard Biometrics at Sea

[56] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf

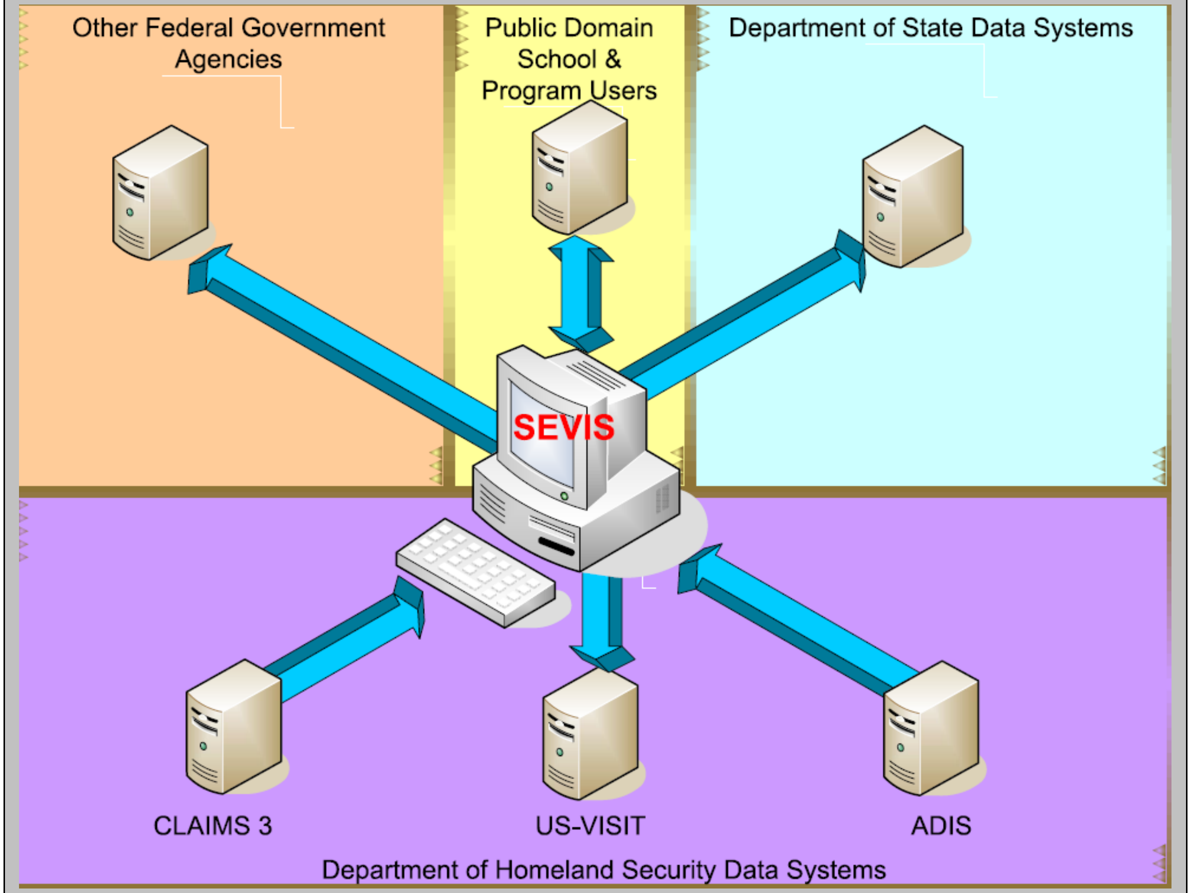
Image Storage and Retrieval System (ISRS) *(Owner USCIS)*

- Image Storage and Retrieval System (ISRS) is a web-based system that permits query and retrieval of biometric image sets and associated biographical data. Indexed data fields include the alien registration number, receipt number, applicants name and date of birth, and card serial number.[57] Image Storage and Retrieval System (ISRS) draws its information from the following sources:
  - CLAIMS 3 is a system that tracks and processes the adjudication of applications and petitions for immigration benefits and services, except asylum and naturalization.[58]
  - CLAIMS 4 is the case processing system for the adjudication of applications for naturalization (N-400).[59]
  - Refugees, Asylum, and Parole System (RAPS) tracks affirmative asylum applications and certain applications for benefits under the Nicaraguan Adjustment and Central American Relief Act.
  - IDENT stores fingerprints and photographs of USCIS applicants.



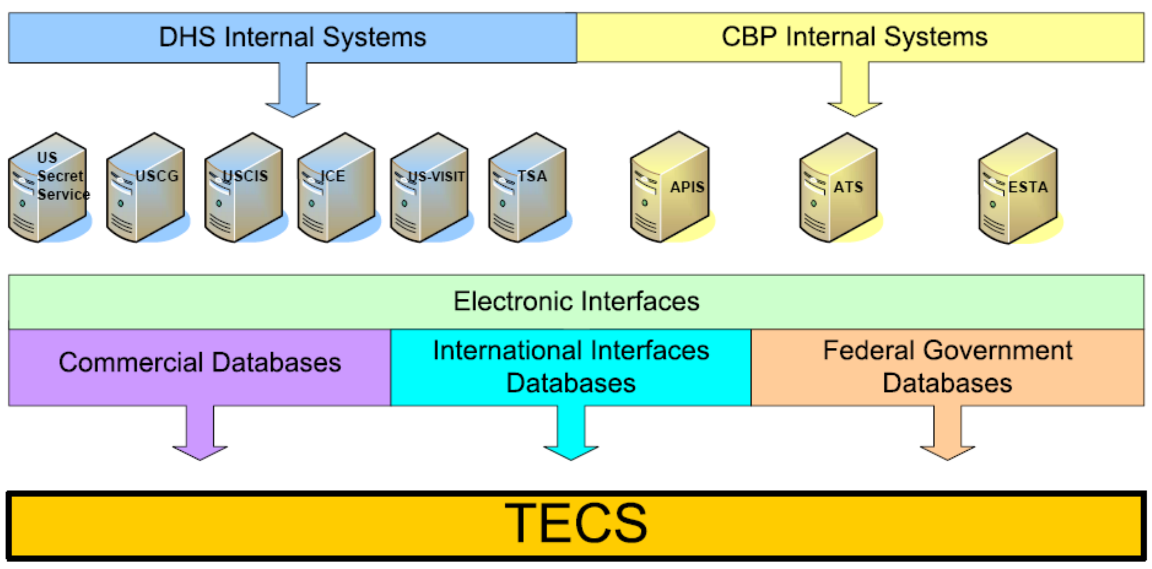
[57] http://dhsconnect.dhs.gov/uscis/org/EXSO/ILink/docView/M450/HTML/M450/0-0-0-7854 html
[58] http://www.dhs.gov/xlibrary/assets/mgmt/e300-uscis-immigra32008.pdf
[59] http://www.dhs.gov/xlibrary/assets/mgmt/e300-uscis-natural42008.pdf

SEVIS *(Owner ICE)*
Student and Exchange Visitor Information System (SEVIS) tracks and monitors information on nonimmigrant students, exchange visitors and their dependents, and on their associated schools and sponsors.


Other Federal Government Agencies
Public Domain School & Program Users
Department of State Data Systems
SEVIS
CLAIMS 3
US-VISIT
ADIS
Department of Homeland Security Data Systems

TECS *(Owner CBP)*

The TECS database contain temporary and permanent enforcement, inspection, and intelligence records relevant to the antiterrorism and law enforcement mission of CBP and other federal agencies. TECS also allows direct access to other major law enforcement systems, to include the Department of Justice National Crime Information Center and the International Justice and Public Safety Information Sharing Network (NLETS).



Appendix F
Major Contributors to this Report

Douglas Ellice, Chief Inspector, Office of Inspections
Lorraine Eide, Senior Inspector, Office of Inspections
Ericka Kristine Odiña, Inspector, Office of Inspections
Pharyn Smith, Inspector, Office of Inspections
Michael Brooks, Inspector, Office of Inspections
LaDana Crowell, Inspector, Office of Inspections

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Policy
Deputy Chief of Staff
General Counsel
Executive Secretariat
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
DHS Component Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;

- Fax the complaint directly to us at (202) 254-4292;

- Email us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.