Department of Homeland Security

Office of Inspector General

Information Sharing on Foreign Nationals: Border Security (Redacted)

OIG-12-39

February 2012

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

Homeland Security

February 13, 2012

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 the Department's information sharing on foreign nationals at U.S. borders. It is based on interviews with employees and officials of relevant agencies and institutions, 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
Acting Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

AMOC	Air and Marine Operations Center
APIS	Advance Passenger Information System
APSS	Asylum Pre-Screening System
BEST	Border Enforcement Security Task Force
CBP	U.S. Customs and Border Protection
Coast Guard	U.S. Coast Guard
DHS	Department of Homeland Security
ENFORCE	Enforcement Case Tracking System
ERO	Enforcement and Removal Operations
FY	fiscal year
GAO	Government Accountability Office

HSI	ICE Homeland Security Investigations
IBET	Integrated Border Enforcement Team
ICE	U.S. Immigration and Customs Enforcement
MOU	memorandum of understanding
NSEERS	National Security Entry-Exit Registration System
OAM	Office of Air and Marine
OFO	CBP Office of Field Operations
OIG	Office of Inspector General
RAIO QA	Refugee, Asylum and International Operations Directorate Quality Assurance
TECS	TECS (not an acronym)
TSA	Transportation Security Administration
USCIS	U.S. Citizenship and Immigration Services
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology

Executive Summary

The Department of Homeland Security has implemented several programs to screen foreign nationals who seek entry into the United States at air, land, and sea ports of entry, as well as persons who seek illegal entry through land and maritime borders. We evaluated whether levels of cooperation, resources, and technology were adequate for department officers charged with border security. This review is the second phase of a three-phase review. We have previously reviewed overseas screening (*Information Sharing on Foreign Nationals: Overseas Screening* OIG-11-68, April 2011).

Some DHS components have developed special-purpose, user-friendly interfaces so that computer users performing focused operations, such as primary inspections at ports of entry, can access DHS databases. However, fragmented data systems and inadequate resources and infrastructure remain a challenge for many officers involved in border security.

Relationships among components work well when they are adequately resourced and their missions are clearly defined. However, some relationships, most notably among law enforcement components on the northern and southern borders, struggle with mission overlap and inadequate information sharing. The U.S. Coast Guard's effective and efficient information sharing approach is an example of how complex multiagency efforts can succeed. However, the sharing of information among other components is still evolving.

We are making eight recommendations to use DHS resources better and facilitate increased data sharing.

Background

DHS OIG Multiphase Review on Information Sharing

This report is the second phase of a three-phase report on information sharing on foreign nationals within the Department of Homeland Security (DHS). In our first report, *Information Sharing on Foreign Nationals: Overseas Screening*, we described extensive DHS efforts to screen foreign nationals before they arrive at a port of entry. Efforts are focused on screening passengers and crew on international flights and sea vessels, as well as maritime interdiction. Overseas screening programs rely on biographical, biometric, and documentary information in DHS and other federal data systems.

In our report, we determined that DHS has improved the evaluation of the admissibility of foreign nationals before they travel to the United States, and that the level of cooperation among DHS components that conduct overseas screening is high. However, we determined that DHS overseas screening initiatives face serious resource and technological challenges. Information is fragmented among more than 17 DHS 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. Although DHS concurred with 17 of the 18 recommendations, 5 recommendations required resources that the programs do not currently have.

In this report, we focus on information sharing among DHS components related to border security. Information sharing within DHS on foreign nationals is the responsibility of five of the seven major DHS operational components, as well as support offices. The operational components are U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), U.S. Coast Guard (Coast Guard), U.S. Immigration and Customs Enforcement (ICE), and the Transportation Security Administration (TSA), each of which is actively involved in sharing information throughout DHS and with other federal, state, local, and tribal partners. Four support offices have 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, two support offices have 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.

In our first report, we reviewed the DHS data systems that are routinely used by DHS officers who are stationed overseas or are stationed in the United States but screen international flights and vessels before embarkation. (See appendix C.) These and other systems will be discussed in this report.

This report evaluates the timeliness and quality of information shared through DHS data systems, and through communication among DHS component agencies. It also discusses how interagency working relationships affect the effectiveness and efficiency of operations to screen and process foreign nationals. We identified agency best practices as well as some of the challenges between agencies to cooperate effectively and share information.

Border Security Operations

Foreign nationals can enter the United States lawfully through any of 327 air, sea, or land border ports of entry. Lawful entry requires CBP Office of Field Operations (OFO) officers to evaluate individuals seeking entry into the United States for compliance with numerous immigration, customs, and agricultural laws and regulations, a process called an immigration inspection.[1] About two-thirds of these inspections involve foreign nationals and about one-third involve U.S. citizens. The CBP OFO National Targeting

[1] http://www.cbp.gov/xp/cgov/border_security/bs/border_sec_initiatives_lp.xml.

Center – Passenger, Passenger Analysis Units at air ports of entry, and joint Coast Guard and CBP maritime operations, conduct advance screening of most international travelers who arrive by air or sea based on passenger or crew manifests. Most noncitizens will have obtained a visa or, if eligible, an Electronic System for Travel Authorization approval to be allowed to travel to the United States and apply for admission at the port of entry.

At land border ports of entry, where CBP officers rarely have advance notice of arrivals, most U.S. citizens and all foreign nationals must present government-issued travel and identification documents. For most nationalities, a passport is required. Since June 2009, U.S. citizens, and citizens of Mexico, Canada, and Bermuda must present a document approved under the Western Hemisphere Travel Initiative.[2] Categories of foreign nationals whose fingerprints are enrolled in the US-VISIT biometric database (Automated Biometric Identification System) have expanded to include most nationalities and visa categories. Fingerprints are now enrolled for many legal permanent residents and citizens of countries for which a visa is not required. Some foreign nationals, such as diplomats and certain northern and southern border crossers, as well as U.S. citizens, are not enrolled in US-VISIT.

In order to protect the United States better after the September 11, 2001, terrorist attacks, foreign nationals from certain countries were required to register with the National Security Entry-Exit Registration System (NSEERS) when they arrived at a port of entry. In 2009, DHS made logistical adjustments necessary to terminate the NSEERS program in the event of a policy change. Data captured in the NSEERS database are transferred automatically to other DHS systems or captured initially in other systems, including US-VISIT and Enforcement Case Tracking System (ENFORCE). DHS encouraged low-threat registrants to obtain waivers for up to one year so they do not have to register each time they enter or depart from the United States. Waivers allow NSEERS registrants to travel for a predetermined period, up to a year, without the need for a CBP secondary inspection for each entry and exit. Ports of entry with a large NSEERS population strongly encouraged frequent travelers to obtain waivers. However, some land border crossings still had NSEERS registrants, including commercial truck drivers and students, who register their entries and exits with CBP as often as twice daily.

[2] http://www.cbp.gov/xp/cgov/travel/id_visa/legally_admitted_to_the_u_s.xml; http://www.dhs.gov/files/programs/gc_1200693579776.shtm.

Although entry and exit registrations have decreased from more than 250,000 in 2002 to about 60,000 in 2010, NSEERS remains a significant CBP caseload. At several ports of entry, NSEERS registrants were the largest caseload handled in secondary inspections.

Most foreign nationals are admitted to the United States after a primary inspection of their travel documents and an assessment of their purpose for traveling to the United States. Travelers whose admissibility cannot be readily determined are referred to secondary inspection for additional checks. A secondary inspection consists of a more detailed review of travel documents and baggage, in-depth questions by a CBP officer, and multiple data checks against various immigration and law enforcement data systems. The outcome of the secondary inspection will generally determine whether the foreign national is permitted to enter the United States. Individuals denied entry may be allowed to voluntarily return to their country of origin or may be detained while their admissibility is determined through formal immigration proceedings. If the foreign national has a visa but is denied entry, CBP will generally cancel the visa at the port of entry.

The following are some general exceptions to these procedures:

- If the local CBP OFO Passenger Analysis Unit or a CBP officer at secondary inspection believes that the case involves terrorist or criminal issues, the case may be referred to ICE Homeland Security Investigations (HSI) or other federal, state, or local law enforcement officers, and the alien, or foreign national, may be subject to criminal prosecution.

- Aliens who express to the CBP officer that they fear to return to their country of nationality because they believe they will be subject to persecution or torture are detained by ICE Enforcement and Removal Operations (ERO). Either CBP, the Coast Guard, or ICE ERO notifies the USCIS Refugee, Asylum, and International Operations Directorate, Asylum Division about these individuals. Asylum officers conduct an interview to determine whether the case has sufficient merit to be referred to an immigration judge for a hearing that would consider granting relief from removal or other protection, such as asylum, deferral or withholding of removal, or relief under

the Convention Against Torture. This process is referred to as the "credible fear" process.

- From August 2002 until April 2011, nonimmigrants from certain predominantly Arab and Muslim countries were required to register under the NSEERS program each time they arrived in or departed from the United States, or had to obtain a waiver of these requirements.

Persons sometimes attempt illegal entry into the United States between land, sea, and air ports of entry, for example across the northern or southern land border, along the coast, or with an unregistered aircraft. Protecting the borders and coasts requires that the U.S. Border Patrol, the Office of Air and Marine (OAM), ICE HSI, and the Coast Guard cooperate with each other as well as with the Canadian and Mexican governments, the military, the Intelligence Community, other federal agencies, and state, local, and tribal governments. Aliens who cannot immediately be removed are referred to the ICE ERO immigration detention system. The U.S. Border Patrol, ICE HSI, the Coast Guard, or ICE ERO may refer detained aliens for a screening interview by an asylum officer for protection issues or a hearing before an immigration judge for other immigration issues, or they may bring criminal charges.

Although the primary focus of this report is on information sharing on foreign nationals who seek to enter the United States, we also reviewed some additional operations that support border security or involve cooperation among the DHS components that participate in border security:

- Although TSA generally does not screen arriving international passengers, it coordinates transportation security systems. Both TSA and CBP are increasingly involved in screening outbound international flights.

- TSA receives assistance from CBP OFO and the Coast Guard with status checks for seaport workers who carry a Transportation Worker Identification Credential. TSA conducts background checks on workers who have unrestricted access to ports before issuing cards.

- The CBP Air and Marine Operations Center (AMOC) provides law enforcement entities with domain awareness information and coordination to support border safety and

security through advance aerial imaging, sensor and tracking systems, and monitoring of general aviation.

- Although ICE ERO detention and removal operations include aliens apprehended within the United States as well as at the border, we reviewed all cooperation efforts between ICE ERO and its DHS partners in this phase of the review.

- Although the USCIS Asylum Division interviews some aliens apprehended within the United States as well as at the border, we reviewed cooperation between the Asylum Division and its DHS partners in this phase of the review.

Results of Review

Infrastructure and Resource Issues Continue To Hinder Information Sharing Efforts

DHS has invested resources in data systems and physical infrastructure to improve information sharing, but some resource needs are unmet. In our report on overseas screening, we noted that information on foreign nationals 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."[3] In this phase of the review, we determined that CBP OFO, the U.S. Border Patrol, and ICE ERO have developed software that consolidates and streamlines access to data for large-scale operations such as primary inspection, border apprehensions, and enforcement and removal. Fragmented data systems remain a challenge for DHS officers who conduct more in-depth evaluations, such as secondary inspections and law enforcement investigations.

We identified two areas in which DHS could conserve resources with relatively minor changes to data systems. (1) The NSEERS program for special registration of certain categories of aliens from predominantly Arab and Muslim countries, and the database that supports this program, is obsolete and should be terminated. (2) CBP could improve productivity in the Passenger Analysis Units by minimizing the number of duplicate flight manifests it receives from commercial airlines. For infrastructure resource needs, although DHS has invested considerable resources to improve

[3] *Information Sharing on Foreign Nationals: Overseas Screening*, Department of Homeland Security, Office of Inspector General (OIG Report-11-68) April 2011.

staffing and infrastructure, many of the ports of entry and land and marine border operations we visited had significant unmet needs. In some instances, resource prioritization by one DHS component affected the efficiency or effectiveness of other components. DHS-level coordination could better prioritize how resources are allocated among components.

Components Seek To Minimize Adverse Consequences of Fragmented DHS Data Systems

Most databases that DHS uses were developed before the Department was created. Each was designed to serve specific antiterrorism, law enforcement, immigration, and traveler screening missions for its creator. The databases are not integrated, and DHS components that screen and vet foreign nationals must check information in as many as 17 data systems.

Three DHS components have developed software to streamline and consolidate necessary information contained in these data systems to assist their officers and agents whose responsibilities for border security are narrowly focused:

- For officers who conduct immigration inspections, CBP has developed software programs that consolidate information from various DHS, Department of State, and Department of Justice data systems. Programs include the Traveler Primary Arrival Client, used for primary inspections at airports, and the Vehicle Primary Client, used for land border crossings. These programs enable the officer to make a timely determination whether a traveler should be admitted or referred for a secondary inspection.

- ICE ERO has developed modules within the ICE system called ENFORCE. This system is used to track immigration enforcement actions and cases. These modules consolidate information necessary to process apprehended aliens, track their immigration proceedings, and assist with removals.

- The U.S. Border Patrol has developed e3, which its Border Patrol Agents use to in-process aliens apprehended on or near the border. e3 has analytic tools that help Border Patrol Agents to assess border security based on patterns of past apprehensions.

However, DHS officers with smaller and more complex border security caseloads experience the same challenges with data systems as do overseas officers and officers at the National Targeting Center – Passenger. These officers include CBP officers in the Passenger Analysis Units at ports of entry, ICE HSI agents, the U.S. Border Patrol agents who conduct investigations, and USCIS asylum officers who evaluate aliens in the credible fear and reasonable fear processes.

The recommendations we made to assist overseas screening in the first phase of our review, *Information Sharing on Foreign Nationals: Overseas Screening*, will also benefit officers charged with more complex border security screening, investigative, and adjudications functions, if funds are obtained.

Terminate the NSEERS Program

After the September 11 attacks, the Department of Justice introduced NSEERS to monitor the arrival, stay, and departure of certain nonimmigrant aliens from predominantly Arab and Muslim countries that were deemed most likely to pose a terrorist threat to the United States. The NSEERS program was transferred to DHS when DHS was created in 2003. Although the program may have had value in the past, advancements in information technology eventually rendered it obsolete.

We intended to recommend that DHS terminate the NSEERS program. Senior DHS officials had been weighing the possibility of terminating NSEERS since at least 2006. On April 28, 2011, while this report was being prepared, it was announced in the *Federal Register* that DHS was effectively ending the program.[4] We support the DHS decision.

Fully implemented in 2004, the US-VISIT Arrival and Departure Information System can track both arrivals to and departures from the United States. In 2009, US-VISIT largely completed its transition from a two-fingerprint enrollment system to a full ten-fingerprint enrollment, a capacity that previously had been most readily available through ENFORCE. Recent expansion of fingerprinting requirements to cover legal permanent residents and nationals from visa waiver countries, as well as the more limited populations in the NSEERS caseload, make US-VISIT the more

[4] *Federal Register* Vol. 76, No. 82, Notices, pp. 23830–23831.

logical system for capturing all biometric information at the ports of entry.

The CBP Automated Targeting System – Passenger and the ICE Pattern Analysis and Information Collection System enable more sophisticated data analysis and intelligence-driven targeting than was available through NSEERS. Both systems can consolidate information about an individual from numerous DHS data systems. Both can also search across data systems for individuals who might match a trend or pattern of concern to the Intelligence Community, such as travel routes or associations with known or suspected terrorists. In addition, CBP can update its targeting software within hours to adjust as the threat environment evolves. In contrast, changes to NSEERS required a lengthy notification process through the *Federal Register*.

Based on our site visits to seven air ports of entry and three land border crossings, we determined that there was no longer a value in the NSEERS program. The ports of entry with the largest NSEERS populations had implemented a 2009 memorandum that enabled CBP to conduct registrations through US-VISIT rather than through the NSEERS database. Many of the smaller ports of entry continued to use the NSEERS database, and struggled with the system's cumbersome design and frequent outages.

Because the NSEERS database is unreliable and it is difficult for NSEERS registrants to adhere to the registration requirements, some waivers were granted on an ad hoc basis. Officials at ports of entry where NSEERS was still used told us that the system frequently did not function properly on some or all computers. We observed that when the NSEERS database functioned poorly, ports of entry issued one-time waivers to registrants and instructed them not to register on their return trip, or issued waivers of the NSEERS registration process to allow registrants to catch flights. However, at some ports of entry, registrants waited until the database resumed functioning, which often took hours. DHS estimates that the cost of NSEERS was more than $10 million annually at its height, though costs became lower with the availability of US-VISIT and waivers.

We also observed that it was difficult for NSEERS registrants with limited English comprehension to understand the instructions for the registration process and the specific NSEERS departure procedures. Although certain ports of entry are not designated to handle NSEERS registrants, officers processed registrants rather

than refer them to the designated port of entry. Several of the secondary inspections we observed involved registrants who had failed to register on their last entry or exit and were processed for a one-time waiver. With so many known improvements needed in the registration system, it is difficult to separate innocent mistakes from intentional violations, which lessens the value of the information collected.

CBP officers also told us that there was little value in the interviews they conducted with NSEERS registrants. NSEERS interviews rely on self-disclosure, and CBP officers noted that information obtained from fingerprints, flight manifests, travel and identification documents, and intelligence sources is more valuable in determining who poses a potential national security risk. CBP officers also noted that the time spent to process NSEERS registrations was an inefficient use of resources. They said that their time could be better spent on more targeted interviews to gather intelligence, identify illegal aliens, or intercept smugglers.

As a result of the DHS action, the program remains in existence after removing from its purview all of the previously listed countries subject to NSEERS registration. Leaving the regulatory structure of the NSEERS program in place provides no discernable public benefit. Deficiencies we identified in the NSEERS program were not related to the composition of the list of subject nationalities, but rather to the insufficient value of the NSEERS data. We encourage DHS to dismantle the vestiges of the program. This will require that DHS initiate a notice and comment rulemaking to eliminate 8 CFR 264.1(f)(2)-(9) and reinstate the prior provisions.

Recommendation

We recommend that the Department of Homeland Security:

Recommendation #1: Fully terminate the National Security Entry-Exit Registration System and reinstate the prior provisions.

Address Duplicate Flight Manifests

CBP Passenger Analysis Units at air ports of entry review flight manifests to identify any potential matches to terrorist watch lists, criminal records, or certain immigration violations. Timely and accurate review of arriving passenger information is critical to border security. During our site visits from August to November

2010, several Passenger Analysis Units reported an increase in the number of duplicate flight manifests. Some duplicate manifests have only slight variations, while other pairs diverge more significantly, such as one variant listing travel document and nationality information that the "duplicate" did not.

We reviewed the range of technical explanations with assistance from CBP's Office of Information Technology. In late December 2010, we conducted a survey of each air port of entry we previously visited. We provided CBP with a copy of the survey responses. The duplicate manifests appear to be related to the transition between existing CBP Advance Passenger Information System (APIS) Quick Query transmissions and the new TSA Secure Flight system. Although all domestic airlines have used Secure Flight for more than a year, and most international airlines made the transition well before the November 2010 final transition, airlines might not have terminated the older APIS Quick Query queue. As a result, some flights and certain commercial airlines are more likely to produce duplicate manifests than others.

Because the Passenger Analysis Units are aware of the problem, the duplicate manifests represent a drain on resources rather than a security risk. Determining which records are duplicates, rather than records of two individuals with similar names, and then determining which record is the most recent and most accurate, adds significant time to the process of vetting inbound flights.

The greatest concern raised at several ports of entry was the difficulty created by the duplicate manifests when placing TECS lookouts on passengers who, for instance, have an outstanding criminal warrant. Lookouts are used to identify certain passengers at primary inspection for possible referral to secondary inspection for a more thorough examination and appropriate action, such as possible arrest. At one port of entry, officials reported that when they placed a lookout on the APIS record that indicated the passenger was on board, it would default to the record that indicated the passenger was not on board, which meant that a primary officer would not be aware of the lookout on the passenger. Officers at ports of entry have developed various alternatives to lessen the possibility that the issue will become a security risk. One port of entry sent CBP officers to meet flights at the gate when there was a lookout on a duplicate manifest. Others had developed procedures to place the lookout against both records within TECS. Nonetheless, passenger screening would be more efficient if the accuracy of flight manifests improved.

Recommendation

We recommend that United States Customs and Border Protection:

Recommendation #2: Collaborate with commercial airlines and develop solutions to reduce the incidence of duplicate flight manifests.

Staffing and Infrastructure Investments

Although DHS has invested considerable resources to improve staffing and infrastructure, some of the ports of entry, land, and maritime border operations we visited had unmet infrastructure needs. In some cases, poor infrastructure affected information sharing among DHS components or had a negative effect on the operations of several components. We identified the following deficiencies and their consequences:

CBP Land Border Ports of Entry

- Limited direct access to law enforcement, intelligence, and immigration databases and high-speed Internet connections
- Insufficient lanes dedicated to the trusted traveler programs to facilitate business and commercial traffic
- Inadequate facilities to segregate aliens who have been referred for a secondary inspection (or more thorough examination) from travelers who seek entry to the United States
- Insufficient space to process passengers from commercial buses within the facility
- Inadequate staff to limit the routine use of overtime

Consequence: Inadequate facilities can slow tourist and commercial cross-border travel without yielding security benefits.

The U.S. Border Patrol – Southern Border

- Unreliable communications infrastructure, such as fiber optic cables for landlines and Internet connections

- Inadequate mobile technology that does not allow agents to access databases to screen aliens in the field

Consequence: Officer safety may be compromised in controlling large groups waiting to be processed and when violent criminals cannot be quickly identified.

ICE ERO Detention and Removal – Detention Space

- Insufficient detention space, especially for juveniles apprehended near the southern border where consular officers from Mexico and Central America are not readily available to facilitate return
- Inadequate detention bed space available to CBP and ICE HSI near the San Ysidro Port of Entry and the San Diego Sector

Consequence: Border security may be compromised if aliens are not detained because suitable bed space is unavailable.

ICE ERO Detention and Removal – Detention Management

- Fingerprinting equipment insufficient or not technologically advanced
- Unreliable high-speed connectivity for data servers
- Limited processing space in detention centers to prepare cases for detention in state and local facilities
- Insufficient ICE ERO staff to transport aliens apprehended by CBP at ports of entry

Consequence: Facility inadequacy slows detention processing and limits the assistance ICE can provide to CBP to manage aliens in custody.

Each DHS component must prioritize among competing demands for staff and infrastructure improvements. One DHS component's choice of priorities may have a direct effect on other DHS components. For example, inadequate ICE ERO staffing and processing facilities require CBP to take greater responsibility to manage and transport aliens in custody. Inadequate family detention is a concern for CBP and ICE HSI, as spouses and children may be

released before issues related to special-interest aliens or potential trafficking victims can be fully evaluated. Centralized oversight of DHS-wide needs and priorities might allocate resources more efficiently.

Coordination Is Essential To Manage the Foreign National Caseload

Several operational components share responsibility for information about, and physical custody of, foreign nationals. In all these circumstances, information sharing is critical to successful border security operations. For example:

- Illegal aliens apprehended by CBP at or between ports of entry may be detained by ICE ERO pending an immigration hearing.

- The Coast Guard, U.S. Border Patrol, and ICE HSI also apprehend illegal aliens at sea or within the United States who may be detained by ICE ERO.

- Some of the aliens apprehended by CBP and ICE request asylum, withholding of removal, or protection under the Convention Against Torture, which requires the USCIS Asylum Division to conduct screening interviews and determinations while ICE ERO detains the applicants.

Overall, we determined that the relationships among the DHS components with shared responsibility are professional and cooperative. However, DHS officers at the sites we visited raised three areas of concern about shared or overlapping missions: (1) The legal documents that ICE ERO receives from ICE HSI and CBP OFO to place foreign nationals in immigration hearings are not always complete; (2) missions that overlap between ICE HSI and the U.S. Border Patrol on the northern and southern border have been a source of concern since the establishment of DHS; and (3) both ICE ERO and asylum officers expressed frustration regarding the length of time required to process some detained asylum cases. DHS-level oversight could address these areas where bilateral efforts have not been successful.

Processing Aliens for Immigration Hearings Requires Interagency Cooperation

CBP OFO, U.S. Border Patrol, the Coast Guard, ICE HSI, ICE ERO, and USCIS Asylum Division have a shared responsibility to

apprehend illegal aliens or place them in legal proceedings before a Department of Justice immigration judge. During our visits, we were told repeatedly that the legal paperwork is a source of frustration. Overall, the transfer of aliens and their legal paperwork between the U.S. Border Patrol and ICE ERO appeared seamless, as both components understood the legal status of the apprehended aliens and use e3 to process aliens subject to removal. Coast Guard processes also worked well. Lines of authority were clearly understood, as the Coast Guard is not limited to enrolling aliens apprehended into DHS data systems based on proximity to shore. Asylum officers noted that other DHS components may not correctly identify whether aliens belong in the asylum, withholding of removal, or Convention Against Torture caseloads, but said that they can easily differentiate the cases based on the information CBP and ICE officers enter in TECS and ENFORCE.

However, ICE ERO officers responsible for detained aliens said that the paperwork from CBP OFO officers and ICE HSI agents is not always complete. Some detention offices did not accept custody of aliens until their legal counsel had reviewed the paperwork for legal sufficiency. This is a source of frustration for staff at the CBP port of entry, which retains custody during this process. Several ICE ERO officers said that the paperwork they received from CBP OFO or ICE HSI was inadequate to place an apprehended alien in removal proceedings, and that ICE ERO spent considerable time amending legal documents before it could present cases to the immigration courts. In a few instances, ICE ERO said that it could not bring charges and had to release aliens because of incomplete paperwork. In most instances, components that experienced difficulty with such shared responsibilities cited a loss of institutional knowledge of immigration law as the cause. In the eight years since the creation of DHS, the percentage of CBP and ICE agents and officers with prior experience in the former Immigration and Naturalization Service has declined because of attrition and retirements.

Each of the components with these shared responsibilities sought to address these deficiencies. They offered to train other components, to provide checklists and point of contact information, and even to process cases themselves. Although these bilateral efforts are commendable, the program would benefit from centralized DHS headquarters-level oversight to resolve training and guidance issues that remain.

Overlapping Missions of U.S. Border Patrol and ICE HSI

One of the primary DHS missions is to secure and manage America's land and maritime borders. According to a 2004 memorandum of understanding (MOU) between U.S. Border Patrol and ICE HSI, the missions of ICE HSI and the U.S. Border Patrol are "intricately connected and complementary."[5] The MOU noted that the U.S. Border Patrol has primary responsibility for all cross-border and border-related interdiction activities between ports of entry and ICE HSI has primary responsibility for all investigations. An addendum to the MOU, signed in February 2007, provided additional guidance that requires U.S. Border Patrol and ICE HSI to familiarize each other with their missions, maintain regular communication, provide notification on potential terrorism issues, use data systems to deconflict cases, and collocate agents to facilitate communication and cooperation.[6]

Despite this guidance, operational challenges between U.S. Border Patrol and ICE HSI remain unresolved. In reviews conducted in 2005 and 2007, we made recommendations to improve coordination and cooperation between the components that either were not adopted or had limited success.[7] In its December 2010 report, the Government Accountability Office (GAO) also raised concerns about systemic U.S. Border Patrol and ICE HSI coordination challenges on the northern border. The GAO report stated that if these issues were not resolved, they could have an adverse effect on border security.[8]

Furthermore, the GAO report stated that current guidance fails to clarify roles and responsibilities or successfully delineate the roles in interdictions and investigations. GAO said that both U.S. Border Patrol and ICE HSI considered the sharing of information between the two agencies to be inadequate, causing duplication of missions and concerns over officer safety. GAO determined that the challenges facing U.S. Border Patrol and ICE HSI underscore the importance of developing and maintaining permanent solutions to mitigate conflicts. GAO also determined that DHS headquarters-

[5] *Guidelines Governing Interaction Between ICE's Office of Investigations and CBP's Office of Border Patrol*, Memorandum from Robert C. Bonner, Commissioner, CBP, and Michael J. Garcia, Assistant Secretary, ICE, November 16, 2004.
[6] *Additional Information on OBP and ICE Negotiations*, Memorandum from Chief Border Patrol Agent David V. Aguilar, OBP 50/1.1.2, February 26, 2007.
[7] *An Assessment of the Proposal to Merge Customs and Border Protection with Immigration and Customs Enforcement* (OIG-06-04); *DHS' Progress in Addressing Coordination Challenges between Customs and Border Protection and Immigration and Customs Enforcement* (OIG-07-38) April 2007.
[8] *Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination Is Needed for the Northern Border* (GAO-11-97) December 2010.

level guidance is needed to provide the oversight and leadership to address these coordination issues.

We conducted our site visits for this review within weeks after the GAO site visits, and included both the northern and southern borders. We concur with the GAO assessment. The unresolved sources of disagreement between ICE HSI and U.S. Border Patrol include the following:

Shared Investigative Territory

Among the challenges both ICE HSI and U.S. Border Patrol agents cited when they conducted interceptions and investigations in the same areas on the northern and southern border are the need to—

- Deconflict access to informants, witnesses, and persons of interest
- Determine when the U.S. Border Patrol intelligence gathering becomes a criminal investigation
- Prioritize controlled cross-border deliveries of drugs, weapons, cash, or aliens operations, which the U.S. Border Patrol leads to support ICE HSI investigations

U.S. Border Patrol Relationships With Department of Justice Law Enforcement Agencies

ICE is the largest investigative branch of DHS and, as noted in the MOU, has primary responsibility for DHS investigations of persons other than DHS employees. (Our office investigates allegations of criminal misconduct by DHS employees.) However, the MOU notes that the U.S. Border Patrol is also authorized to conduct investigations. This overlap is not unique; other federal agencies, notably the Department of Justice, are authorized to conduct investigations that overlap with the DHS mission. In this structure, the missions of ICE HSI and the U.S. Border Patrol are not well aligned:

- Although the U.S. Border Patrol moved from the Department of Justice into DHS in 2003, it remains bound by a 1996 MOU to refer all of its drug seizures first to the Department of Justice Drug Enforcement Administration when such seizures are made under the authority of its Title 21 designation.

- The U.S. Border Patrol has well-established relationships with Department of Justice agencies whose missions overlap with ICE's on the northern and southern borders, such as the Federal Bureau of Investigation and the Bureau of Alcohol, Tobacco, Firearms and Explosives. Because of these established relationships, these agencies often ask the U.S. Border Patrol directly for information and assistance rather than work through ICE HSI.

- ICE's mandate is broad, and includes issues in the U.S. Border Patrol's mandate (e.g., national security threats, human smuggling and trafficking, and narcotics smuggling) as well as issues outside its direct mandate (e.g., financial crimes, commercial fraud, counterproliferation, child pornography and exploitation, and immigration benefit fraud).

Information Sharing Constraints

Information sharing on potentially overlapping operations is a source of disagreement between the U.S. Border Patrol and ICE HSI. Both are concerned that gaps in information sharing practices could compromise officer safety:

- The U.S. Border Patrol expected more situational intelligence from ICE HSI than it currently receives and generates its own intelligence to fill this gap.

- The U.S. Border Patrol expected more information from ICE HSI on open investigations, particularly on cases for which the U.S. Border Patrol provided the original lead, but ICE HSI considers that information on open investigations should be shared on a "need to know" basis.

- Data entry in TECS is an ineffective method for sharing information, as the U.S. Border Patrol does not have access to the TECS investigative module, and ICE HSI considers some Border Patrol case information to be delayed or incorrectly entered into TECS.

Data System Constraints

The current structure and planned upgrades to the data systems are not designed for information sharing on investigations and operations that may overlap:

- The U.S. Border Patrol's primary data system is e3, an ICE-owned biometric-based system used to track apprehensions, detentions, immigration hearings, and removal of illegal aliens.

- ICE HSI's primary data system is TECS, a CBP-owned biographic-based system designed to track activities at ports of entry, seizures, and (in the TECS III module) ongoing investigations.

- The U.S. Border Patrol created e3, intended for use by both ICE HSI and U.S. Border Patrol for border operations. However, ICE has not adopted the system.

- Both ICE HSI and the U.S. Border Patrol expressed concern that TECS modernization led by the CBP Office of Information Technology did not solicit adequate comments on their information sharing needs.

The GAO December 2010 report recommended DHS-level oversight of U.S. Border Patrol and ICE HSI compliance with the provisions of the interagency MOU, to include evaluation of outstanding challenges and planned corrective actions. DHS concurred with the recommendation, but said it would comply by reconstituting the former ICE-CBP Coordination Council, which met for a few years after our 2005 report and then became inactive, to review compliance. GAO noted that while it existed, the Coordination Council "was unable to improve upon the long-standing coordination challenges between U.S. Border Patrol and ICE HSI."[9] Many U.S. Border Patrol and ICE HSI agents we interviewed also expressed concern that enforcement of the MOU, even through a Coordination Council, would not address long-standing sources of disagreement. Most said the solution was clear DHS-level guidance on missions and priorities.

[9] *Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination Is Needed for the Northern Border* (GAO-11-97) December 2010.

We believe that GAO's recommendation, if implemented as envisaged, would address many of the tensions between the U.S. Border Patrol and ICE HSI. We consider that duplication of effort, poorly aligned priorities, inadequate methods to share and safeguard information, and potential threats to officer safety will continue until DHS-level oversight of the MOU is addressed.

Recommendation

We recommend that the Department of Homeland Security:

Recommendation #3: Establish Department-level oversight to address Customs and Border Protection, Office of Border Patrol, and Immigration and Customs Enforcement, Homeland Security Investigations operational challenges.

Improve Timeliness of the Reasonable Fear Process

The asylum pre-screening program also requires cooperation between DHS components. The USCIS Asylum Division has jurisdiction for two categories of aliens who seek protection after being apprehended by CBP or ICE and detained by ICE ERO.

One category is aliens who seek asylum when they are detained at a port of entry by CBP OFO or are apprehended by U.S. Border Patrol. Asylum officers determine whether these applicants have a "credible fear" of persecution or torture if they are returned to their country of nationality. The credible fear standard has a low threshold to determine whether the case can be referred to an immigration judge for a full asylum hearing: 67% of applicants pass the screening standard. (See appendix D.) The forms of relief from removal available to credible fear applicants include asylum status (which can lead to lawful permanent resident status), withholding of removal, or relief under the Convention Against Torture.

The second category is aliens who are not eligible for asylum but might be entitled to other forms of relief, such as withholding or deferral of removal. Asylum is not available to aliens who have a prior order of removal that is reinstated when they are apprehended or have been convicted of an aggravated felony in the United States. Some of these aliens are detained at a land border by U.S. Border Patrol or OAM; port of entry by CBP OFO; or along the coast by the Coast Guard. They may also be apprehended within the United States by other means, such as enforcement actions by

ICE HSI, or transfer from federal, state, or local prisons to ICE ERO custody for removal. If the aliens express a fear of persecution or torture after apprehension, they are referred to the asylum office for a "reasonable fear" determination.

In the past year, there has been an increase in the number of reasonable fear cases, which asylum officers said might be a result of increased interior enforcement efforts by ICE. Asylum officers determine whether these applicants meet the reasonable fear standard, which has a higher threshold to determine whether the case can be referred to an immigration judge: 24% of applicants meet the screening standard. (See appendix D.) The forms of protection available to the reasonable fear caseload, if granted by an immigration judge, are generally intended to be temporary, until conditions in the country of nationality improve or a third country agrees to take the alien.

Overall, relationships between the USCIS Asylum Division and its partners in CBP OFO, U.S. Border Patrol, ICE HSI, and ICE ERO are positive. Asylum officers told us that they are confident that CBP and ICE officers refer cases where the individual has expressed a fear of return, as well as some discretionary cases based on country of origin or unusual behavior. At the local level, each asylum office we reviewed offered training to CBP and ICE officers on recognizing potential cases. CBP and ICE officers we interviewed were familiar with the forms, procedures, and notification processes for asylum cases. Asylum offices had also developed information sharing mechanisms such as group mailboxes, checklists, and regular meetings to support the notification process. Asylum officers said that ICE officers readily facilitated interviews and would provide security for interviews with potentially violent applicants.

We determined that the Asylum Division generally processes ICE ERO detainees for credible fear screening expeditiously. The Asylum Division strives to make a decision within 14 days of notification by ICE or CBP for at least 85% of cases. Based on data the Asylum Division provided us, from June 1, 2005, to June 30, 2010, credible fear determinations were completed within 14 days at least 90% of the time. Asylum Division headquarters reviews all credible fear denials, but only reviews grants and withdrawals in certain circumstances.

In contrast, both field asylum officers and ICE ERO officers expressed frustration with the time it takes the Asylum Division to

complete reasonable fear cases. During our fieldwork, there were no timeliness standards for completion of reasonable fear cases. Asylum officers said that with limited resources and no set deadlines, the Asylum Division delays reasonable fear interviews to keep current with other caseloads. Of the 4,532 reasonable fear cases processed from June 1, 2005, to June 30, 2010, asylum officers noted a delay caused by inadequate resources in 1,307 cases, or 29%. Cases with available data took an average of 72 days to complete, and 24% took more than 3 months to complete. (See appendix E.)

In light of these timeliness issues, the ability of the Asylum Division to track reasonable fear case completions is essential. It is generally understood that the Asylum Division considers a reasonable fear case complete when the decision is served on the applicant by the Immigration Court, as indicated by the "Decision Served" field in the Asylum Pre-Screening System (APSS), but current reasonable fear procedures do not provide explicit instructions for APSS entries for all data fields. Improvements in data entry procedures could result in more effective overall case management, specifically in the areas of timeliness and completions. In particular, the procedures should direct users to use the date of service ("Decision served" in APSS) to communicate completion of the reasonable fear case (i.e., service of the positive or negative decision on the detainee, on ICE ERO, and on the Immigration Court) or to use the date the case is administratively closed ("Close Effective" date in APSS.)

Each of the five asylum offices we visited identified the headquarters review process as a source of delay for completing reasonable fear cases. Asylum officers said that the quality assurance program was inadequately staffed for the sharp increase in reasonable fear cases, and that it prioritized credible fear cases over reasonable fear cases. At the time of our fieldwork, only credible fear denials were reviewed, but headquarters reviewed 100% of grants, denials, and withdrawals for reasonable fear cases. For cases with available data, the headquarters review process for reasonable fear cases took an average of 29 days to complete. (See appendix E.) Information on how long the review process took for the remaining cases, including withdrawals, was not available.

ICE officers at the detention facilities expressed frustration with the amount of time it took to resolve cases in the Asylum Division's jurisdiction. One concern was with detainees who had asked to withdraw their applications to remain in the United States

and awaited permission to return home pending legal disposition of their case. Some of this population are discontented about their continued detention and are disruptive to other detainees. ICE officers said that the daily cost of detention for each detainee can range from $60 to more than $200. To detain an asylum applicant for a month without an interview in addition to another month without a final decision is an inefficient use of detention bed space. Since asylum officers cannot predict with any certainty how long each case will take, they cannot provide this information to ICE ERO.

With limited asylum resources and no timeliness requirements, Asylum Division delays in the reasonable fear caseload are a likely result, but ICE ERO bears the costs of such delays. The Asylum Division has tried to reduce delays before the initial interview. Asylum officers are assigned permanently to some facilities with a large caseload. Although asylum officers may schedule interviews with less delay by video-teleconference, video-teleconferences place an administrative burden on ICE ERO resources. During video-teleconferencing interviews, at several points ICE ERO officers must obtain and share files, receive faxed documents, obtain signatures, and return completed faxed documents.

Timely interviews will have limited effect unless delays in the headquarters review process are also addressed. In January 2011, the Asylum Division issued two memorandums on the reasonable fear process. The first memorandum instituted processing criteria for reasonable fear cases that are similar to those used to measure the credible fear cases. All negative determinations are still reviewed, but only a sampling of positive determinations is taken.[10] The second memorandum pertained to applicants who have requested to withdraw their application. For these cases, new headquarters review criteria for reasonable fear cases are now comparable to the prioritized review criteria for credible fear cases. Headquarters review is not required before the applicant is allowed to withdraw, and quality assurance will be conducted on closed cases.[11] Headquarters officers said that a goal for fiscal year (FY) 2011 was to identify timeliness criteria for the reasonable fear caseload. Asylum officers indicated that headquarters was developing a methodology to set these criteria.

[10] *Revised Reasonable Fear Quality Assurance Review Categories*, Memorandum from Joseph E. Langlois, HQRAIO 120/12.16a., January 10, 2011.
[11] *Further Revised Reasonable Fear Quality Assurance Review Categories*, Memorandum from Joseph E. Langlois, HQRAIO 120/12.16a., January 28, 2011.

We believe that the increased use of video-teleconferencing and the streamlined headquarters quality assurance process are key to improving the timeliness of reasonable fear adjudications. Field site visits by headquarters officers responsible for quality assurance and program management may assist in identifying training and guidance needs and in developing a practical methodology to set timeliness criteria.

Recommendations

We recommend that United States Citizenship and Immigration Services:

Recommendation #4: Establish timeliness criteria for completing reasonable fear cases.

Recommendation #5: Record in the Asylum Pre-Screening System database the date when each reasonable fear case is returned to U.S. Immigration and Customs Enforcement jurisdiction.

Multilateral Support Is Developing for Information Sharing

Information sharing on foreign nationals at ports of entry and along the land and maritime borders is primarily the responsibility of the CBP Office of Field Operations, U.S. Border Patrol, ICE HSI, ICE ERO, the Coast Guard, and the USCIS Asylum Division. These components have legal authority and access to biometric and biographic data systems necessary to decide who is admitted or denied admission to the United States, apprehended and placed in immigration or criminal proceedings, or ultimately removed from the United States. As the December 2010 GAO report noted, many task forces, joint operations, and working groups led by ICE and CBP play a fundamental role in information sharing on foreign nationals and could be better coordinated. We reached the same conclusions. In addition, we observed that other DHS components have developed a geographic-based role, which is essential to coordination and communication on foreign nationals at ports of entry and land and maritime borders. Although the Coast Guard's role in coordination and facilitation of law enforcement and interception activities in the maritime environment is the most complex of the components, its partners gave Coast Guard uniformly high marks for its information sharing. TSA's role has expanded rapidly at commercial air ports of entry. TSA's Coordination Centers are an innovative contribution to information sharing, but TSA involvement with foreign nationals at air ports of entry

continues to evolve. Although the CBP AMOC under the OAM has a long history of support for border enforcement, its potential has not been fully developed.

CBP and ICE Border Security Operations Would Benefit From DHS-Level Oversight

We described earlier the difficulties that arise from the overlapping mandates of CBP and ICE, and the insufficient oversight and direction available from DHS. Similar issues diminish the effectiveness of two interagency forums: the Integrated Border Enforcement Team (IBET) and Border Enforcement Security Task Force (BEST).[12] IBET is a cooperative binational initiative that secures the border between Canada and the United States by identifying, investigating, and interdicting persons, organizations, and goods that are involved in organized criminal activity.[13] BEST is a binational forum led by ICE to identify, disrupt, and dismantle criminal organizations that pose a significant threat to border security.[14] In its December 2010 report on northern border security, GAO concluded that these forums have enhanced information sharing, but also compete for resources and have overlapping missions and areas of operation. GAO noted that northern border partners cited challenges to allocate sufficient resources for the growing number of interagency forums that have been established in their geographic area of responsibility.

Based on our site visits and interviews with the U.S. Border Patrol and ICE personnel on the northern border, we share GAO's conclusions. On our site visits to the southern border, where there is no IBET presence, similar concerns were expressed about how to staff the BEST task forces and the activities of an ICE-led mission. Although DHS attempts to maximize its presence on the northern and southern borders through interagency forums, concerns were raised regarding duplication and overlapping missions. Some of the ICE HSI and the U.S. Border Patrol agents we interviewed in the field and at headquarters said that the only way to address tensions between ICE HSI and the U.S. Border Patrol is by establishing clear DHS-level guidance on missions and priorities.

The GAO December 2010 report recommended that DHS provide DHS-level guidance and oversight for interagency forums

[12] *Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination Is Needed for the Northern Border* (GAO-11-97) December 2010.
[13] http://www rcmp-grc.gc.ca/ibet-eipf/index-eng.htm.
[14] http://www.ice.gov/best/.

established or sponsored by its components to ensure that the missions and locations are not duplicative and to consider the downstream burden on northern border partners.

DHS concurred with this recommendation, but said that the structure of the Department precludes accomplishing the goal of DHS-level guidance and oversight through a single headquarters organization. It said that through strategic and operational planning efforts, DHS will review the inventory of interagency forums to assess efficiency and identify challenges. GAO responded that it encouraged DHS to "provide the guidance and oversight necessary" to mitigate duplicative efforts.[15]

We believe that GAO's recommendation, if implemented as GAO envisaged, would address many of the tensions between the U.S. Border Patrol-coordinated and ICE HSI-led interagency forums on both borders. Direct DHS-level guidance and oversight is necessary to establish clear goals and priorities to facilitate cooperation and coordination.

U.S. Coast Guard Provides Information and Support When Coordinating With Multiple Agencies

With the exception of its migrant interdiction mission, the Coast Guard's role in information sharing on foreign nationals is an indirect consequence of its missions to defend ports, waterways, and coastal areas; conduct search and rescue operations; and conduct drug interdiction. Nonetheless, the Coast Guard's strategy to fulfill its missions has made it an integral component of DHS information sharing on foreign nationals in the maritime environment.

The Coast Guard has established efficient and effective programs and processes to share information among DHS components when they encounter foreign nationals at sea ports of entry. The Coast Guard has stations at most of the coastal and maritime locations that are critical to border security, including the rivers and Great Lakes that separate the northeastern United States from Canada, and major coastal cities such as Miami, New York City, San Diego, and Seattle.

The Coast Guard has developed collaborative information sharing relationships with other DHS components and interagency

[15] *Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination Is Needed for the Northern Border* (GAO-11-97) December 2010.

partners. At each coastal and maritime site we visited, the Coast Guard played a key role in facilitating joint law enforcement operations. Central to the success of these operations is that they host multiagency partnerships that are located onsite to enhance information sharing capabilities. For example, at major ports, such as New York City, San Diego, and Seattle, the Coast Guard facilitates Joint Harbor Operations Centers. These centers coordinate as many as 50 federal civilian and military, state, local, and business entities involved in commercial and recreational maritime transport and in provisions for safety and security. In the Los Angeles/San Diego area, the Coast Guard hosts the Maritime Unified Command, an innovative multiagency partnership that facilitates information sharing and coordination with multiple agencies on missions related to maritime activities.

The Coast Guard and CBP pool resources to assess passengers and crews of cruise and cargo ships. The Coast Guard receives manifests of passengers and crews of vessels via the Ship Arrival Notification System, and works with CBP OFO to screen and cross-check information against CBP data systems, such as TECS. The Coast Guard has jurisdiction to board vessels to conduct safety and security checks, and routinely brings CBP OFO officers on board to assist with the evaluation of passengers and crew. With CBP on site at Joint Harbor Operations Centers and Coast Guard Stations, the Coast Guard can obtain timely information on foreign nationals from a broad range of databases.

As much through voluntary integration as through regulatory requirements, the Coast Guard has become an essential element of information sharing on foreign nationals. At harbors and ports, the Coast Guard assists TSA with the examination of Transportation Worker Identification Credential cards issued by TSA to workers who have unescorted access to secure areas of ports and harbors. The U.S. Border Patrol works closely with the Coast Guard to identify persons rescued or apprehended at sea. The Coast Guard provides logistics and vessels for many joint investigative and interception activities on the northern and southern maritime borders, such as joint operations by the U.S. and Canadian governments to board vessels, IBET interception operations, and BEST investigations.

Through its coordination centers and joint operations, the Coast Guard has enhanced information sharing on foreign nationals. At each site we visited, CBP and ICE praised the Coast Guard for its ability to both organize command and communication facilities

and work cooperatively in shared areas of responsibilities. Both the Coast Guard and its partners identified the Coast Guard's clearly delineated role at maritime borders as a central reason for its success in joint operations: Although the Coast Guard may apprehend foreign nationals, it partners with CBP or ICE to determine their status.

TSA Coordination Centers Provide Real-Time Readiness and Awareness

TSA Coordination Centers play an increasing role in information sharing on foreign nationals in commercial airports. The centers are a 24/7 information hub for the majority of TSA's operations, with national real-time information sharing through the Domestic Event Network and a dedicated telephone network that links the centers. The Domestic Event Network enables TSA officers to listen to events nationwide as they happen and determine quickly whether an event is an isolated local incident or a coordinated disruption. The centers are one-stop shops for information used by TSA and its federal, state, and local agency partners.

Transportation Security Officers screen information in real time from available data systems, evaluate the information, and determine any interrelationships, including those that relate to the affected transportation modes.

Each Coordination Center uses a system of notification matrices to distribute information on all incidents that occur at the airport. The notification matrix is a quick reference guide for Transportation Security Officers to determine the component and method to contact based on the severity of the incident. The notification matrix is developed in cooperation with the component that receives the notification. For example, CBP OFO can specify that it wants immediate telephone notification for a no-fly match, while ICE HSI can specify that it would prefer email notification after the fact for routine confiscation of weapons. The notification system has reduced information sharing stovepipes and formalized appropriate incident response.

Nonetheless, we observed major challenges at some of the Coordination Centers. Staffing has not increased commensurate with the additional workload from the expansion of the no-fly watch lists in early 2010. [redacted]

Recommendations

We recommend that the Transportation Security Administration:

Recommendation #6: Provide all Coordination Centers with live video feeds from security cameras in the airport terminals.

Recommendation #7: Provide all Coordination Centers with access to federal law enforcement data systems.

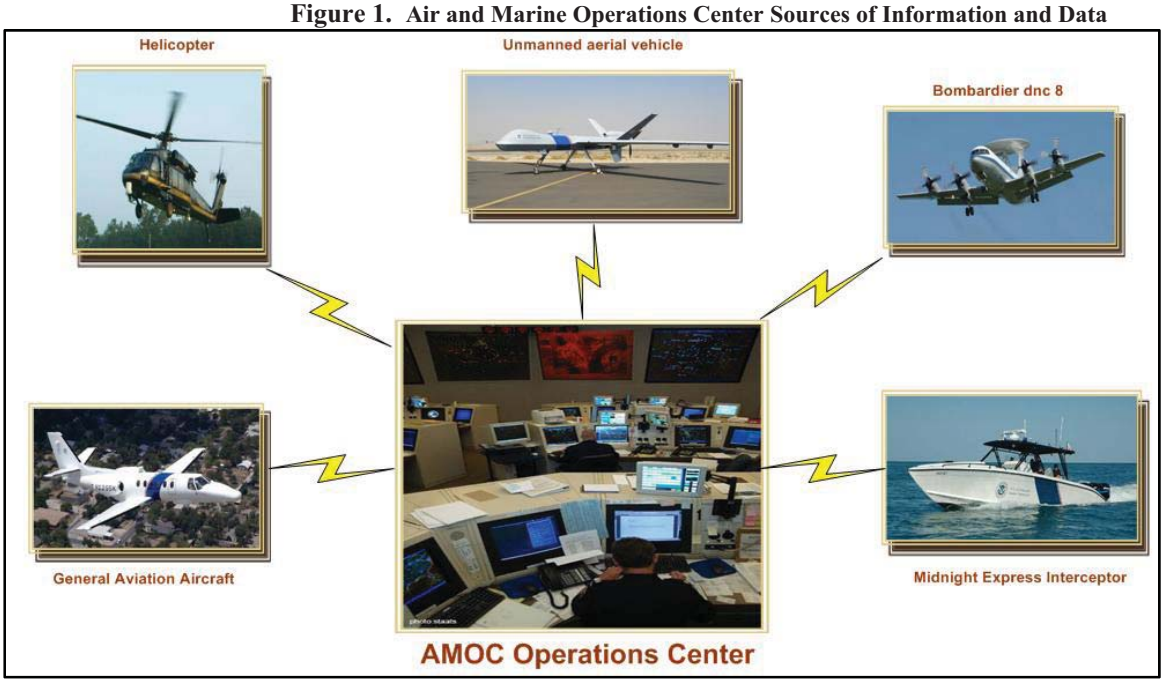
Increased Outreach Effort Is Needed at the Air and Marine Operations Center To Advance Current and Future Expansion Initiatives

The AMOC, in Riverside, California is an operational domain awareness center within CBP OAM. The center was established in 1988 as a state-of-the-art law enforcement radar surveillance center to counter the threat of airborne drug smuggling.

Although OAM, including the AMOC, has limited involvement screening foreign nationals, the information that the center provides to enforcement officers is valuable to border security. The center has a wide range of responsibilities that include detection and coordination efforts for OAM. The center also provides aerial coverage during natural disasters and humanitarian relief efforts, [redacted] and assistance to the U.S. Secret Service with fly-over operations for national special security events.

The technologies that enable the center to provide such support include a surveillance system capable of integrating an extensive network of ground-based and airborne radar, aerial imaging, and streaming video and data from manned and unmanned aerial surveillance vehicles, which can observe and record aircraft and cross-border activity. Figure 1 illustrates some of the information and data sources the AMOC uses.

Figure 1. Air and Marine Operations Center Sources of Information and Data



Source: CBP Air and Marine, Federal Aviation Administration Unmanned Aircraft System Tech Conference[16]

The center's database includes all registered flights and is therefore able to identify unregistered flights and flights that do not follow their registered flight plan. The center observes more than 1,000 flights a day and can closely track small aircraft that have anomalous flights. The center also has some ability to track ships in U.S. territorial waters.

With these capabilities, the center is uniquely qualified to support CBP, ICE, and other law enforcement entities with information sharing on foreign nationals who attempt to enter or exit the United States illegally between ports of entry. Illicit cross-border activities may involve smuggling drugs, cash, and weapons, as well as human trafficking. When the center identifies a plane with an unregistered flight plan, OAM launches aircraft to classify the target of interest. It also, if necessary, coordinates with ICE HSI or the U.S. Border Patrol to check whether the flight termination is a drop-off for contraband or illegal aliens. When OAM identifies individuals crossing the border between ports of entry, the center can notify the appropriate law enforcement organization of their approximate location so they can be apprehended. If ICE plans to prepare a court case that involves alien smuggling or trafficking,

[16] CBP Air and Marine, FAA UAS Tech Conference, January 2007. http://www faa.gov/news/conferences_events/new_tech_2007/presentations/media/day2/pitts.ppt.

the center can provide radar and video surveillance footage captured by OAM aircraft as forensic evidence. The center can also notify law enforcement entities of the presence of an unidentified ship in U.S. territorial waters.

The center has offered its services and resources to components within and outside DHS. The center's wealth of information, expertise, and resources can be a valuable asset to DHS components and other border security agencies. The information available to the center through its radar surveillance and access to detailed video imagery is an information sharing force multiplier for other law enforcement officers in their investigations and interceptions of foreign nationals.

Despite these assets and information sharing efforts, DHS components do not fully understand or use the center's capabilities. Center officials told us that although it has primary responsibility to monitor general aviation, more than 50 international, federal, state, and local agencies are involved in air domain activities, and these agencies do not always communicate and coordinate effectively. Even within the federal government, although the center has developed a complementary relationship with the Drug Enforcement Administration-led government-wide El Paso Intelligence Center, it had to deconflict overlapping missions with a newly developed intelligence section in the TSA Transportation Security Operations Center.

Overall, the center has established effective relationships with the U.S. Border Patrol and ICE HSI when they request assistance on a specific interception or investigation. However, when the center develops its own leads based on suspicious flight patterns or border crossings, it may contact several DHS entities, as well as other federal, state, and local partners, to find a law enforcement organization with resources to follow through on the information.

Center officials and liaisons said that their capabilities are not widely known throughout all the other DHS components. They also told us that the center's role to monitor general aviation and assist in investigations is not widely understood. Officials said that their efforts to promote their capabilities and services to other federal, state, local, and tribal law enforcement entities have had limited success. Center employees also told us that their priorities and mission are not well defined or well aligned with those of the DHS components and other agencies they support. The center has experienced difficulty recruiting liaisons and balancing its needs

with those of the liaisons' home agencies. Some officials expressed the opinion that its operations would be better utilized if the entire air and marine program were directly under DHS leadership.

Most DHS joint operations are housed within one DHS component, and some, such as the Coast Guard operations discussed above, are quite successful. We therefore do not recommend that the AMOC be relocated within DHS. However, we consider that CBP could, at the headquarters level, provide additional support to the center's outreach efforts to become more useful in border security and information sharing initiatives. We also believe that the center would benefit from DHS-level guidance in establishing priorities and better defining the role of DHS liaisons.

Recommendation

We recommend that United States Customs and Border Protection:

Recommendation #8: Provide federal law enforcement agencies updated training or guidance on the operational capabilities the Air and Marine Operations Center offers to support border security initiatives.

Management Comments and OIG Analysis

A copy of the Department response is included as appendix B. The Department concurred with five of our eight recommendations. A summary of the Department response to each recommendation, and our analysis, is included below.

Recommendation #1: Fully terminate the National Security Entry-Exit Registration System and reinstate the prior provisions.

Management Response

The Department said that the Secretary's authority, as exercised under the NSEERS regulations, is broader than the information collection program based on country designation described in our draft report. The Secretary has chosen to retain this regulatory framework to enable prompt action to require registration of a category or categories of aliens, if necessary, through rapid publication of a *Federal Register* Notice. The Department noted that the retention of this regulatory framework has no direct cost to

the Department, while a formal rulemaking to rescind the regulations would be costly and time consuming, with the possibility that additional costly and time-consuming rulemaking would be necessary if registration were needed in the future. The Department would keep the regulation in place to ensure that the Secretary retains the authority in case it is needed in the future.

OIG Analysis

The Department did not concur with Recommendation #1. We determined that the Department is making a reasonable policy determination to maintain the existing regulatory framework. However, there are deficiencies and inefficiencies in the data system that was established to track NSEERS data. The availability of newer, more capable, DHS data systems argues against ever utilizing the NSEERS data system again. It is possible that the Department does not disagree, and is simply preserving the NSEERS regulatory framework, but would employ the modern data systems if it decides someday to require the initiation of some new kind of registration program.

Recommendation #2: Collaborate with commercial airlines and develop solutions to reduce the incidence of duplicate flight manifests.

Management Response

The Department concurred with Recommendation #2. CBP has implemented the Flight Close Out message process whereby carriers are required to identify who is on the aircraft. CBP described the process as reconciliation of the APIS records transmitted and distinguishing passengers on board the aircraft from those who were transmitted but did not board the aircraft. CBP said this effort assists the officers in identifying which set of biographic information should be used in the screening process. The changes are designed to enhance the officer's ability to screen the correct manifest entry by identifying which set of information represents the traveler on board the aircraft; correcting the system error that prevented lookouts from displaying when duplicated manifests entries existed; and removing from primary processing the records of passengers identified as not on board to ensure that officers are processing only the screened passenger data.

OIG Analysis

CBP's actions are consistent with the intent of the recommendation. In the corrective action plan, CBP should

provide further details of the discussions with commercial airlines to reduce the incidence of duplicate flight manifests. A collaborative approach with commercial airlines is necessary. CBP relies on the information submitted by commercial airlines to conduct the screening process. Additional information that might be included in the corrective action plan includes the following:

- The status of resolving the duplicate flight manifests problem identified in the OIG report;

- Whether terminating the transmittal of information via APIS Quick Query will eliminate duplicate flight manifests; and

- Information as to whether officers can submit multiple lookouts via TECS on the same passenger with a different passenger record or unique locator.

Recommendation #3: Establish department-level oversight to address Customs and Border Protection, Office of Border Patrol, and Immigration and Customs Enforcement, Homeland Security Investigations operational challenges.

Management Response

The Department concurred with Recommendation #3. The Department stated that it exercises its oversight and coordination responsibility through a variety of forums. These include the Information Sharing Governance Board; the Department's Law Enforcement Information Sharing Initiative Executive Director; and the Interagency Northern Border Counter Narcotics Strategy. Both the U.S. Border Patrol and ICE HSI will implement the following corrective actions:

- Regular collaboration on quarterly joint intelligence threat assessments by geographic area to identify and prioritize specific threats common to both agencies;

- Joint operational planning to disrupt and mitigate priority threats identified in the threat assessments;

- Formalization of a joint information and data sharing protocol, to include shared access to agency-specific data systems; and

- Identification of specific objectives within Customs and Border Protection to bridge the identified gaps between intelligence gathering and operations requiring short-term investigations.

OIG Analysis

We believe that the Department's effort will improve coordination between the U.S. Border Patrol and ICE HSI. In the corrective action plan, please provide, for each of the four areas listed above, the following: copies of memorandums, meeting minutes, intelligence and strategic planning reports, threat assessments, and any other evidence.

Recommendation #4: Establish timeliness criteria for completing reasonable fear cases.

Management Response

The Department concurred with Recommendation #4. The Department stated that in FY 2011, Headquarters Asylum established a performance measure that 85% of reasonable fear cases must be completed within 90 days beginning with the referral date of the case from ICE ERO and ending with the case completion date within the Asylum Office. Also, an additional performance measure requires that 95% of pending reasonable fear cases must not be pending for more than 150 days and that updates be provided every 30 days thereafter regarding the progress on resolving the issues preventing decision issuance.

For FY 2012, Headquarters Asylum has developed two initiatives. The first initiative will implement Refugee, Asylum and International Operations Directorate Quality Assurance (RAIO QA) review of reasonable fear determinations and pilot RAIO QA review of credible fear determinations. The second initiative consists of implementing the two performance goals stated above. In addition, Headquarters Asylum plans to modify APSS, reasonable fear procedures, and weekly reports in order to further standardize APSS data entry and to assist Asylum Offices with the timely completion of reasonable fear determinations.

OIG Analysis

In the corrective action plan, please provide the FY 2012 annual memorandum to Asylum Office Directors outlining each Asylum Office's performance objectives for the fiscal year to improve the processing of reasonable fear determinations.

Recommendation #5: Record in the Asylum Pre-Screening System database the date when each reasonable fear case is returned to U.S. Immigration and Customs Enforcement jurisdiction.

Management Response

The Department did not concur with Recommendation #5. During the fieldwork stage, we identified a perceived data deficiency in the APSS database resulting in the Asylum Division being unable to assess reasonable fear case completions. After the exit conference, we requested clarifications on the data field determined to be deficient. USCIS said that it has a method to record and assess reasonable fear timeliness and completions.

OIG Analysis

USCIS believes that alternate data entry capabilities and recently implemented procedural changes are responsive to the intent of the recommendation. The action the Asylum Division describes does not specify whether Asylum Officers are recording when each reasonable fear case is returned to ICE jurisdiction within the APSS database. In the corrective action plan, please provide copies of the data fields within APSS and procedures requiring Asylum Officers to complete the data fields necessary to track timeliness and completions of reasonable fear determinations. Upon receipt of the corrective action plan, we anticipate closing this recommendation.

Recommendation #6: Provide all Coordination Centers with live video feeds from security cameras in the airport terminals.

Management Response

The Department concurred with Recommendation #6. The Department said that the Coordination Center is the primary communication hub for all TSA activity within the Federal Security Director domain. The Department recognizes that the Coordination Centers play an important role in information sharing on foreign nationals in airports. The Department reported that access to closed-circuit television is coordinated on the local level through TSA, airport operator, and other entities with a need to know. However, because TSA does not own the closed-circuit television equipment, granting access to the Coordination Center is logistically challenging. The Department stated that in order to fully maximize the Coordination Centers' one-stop shop of information for TSA and its federal, state, and local agency

partners at the local level, TSA will consider the resources available and whether or not it can expand such access.

OIG Analysis

In the corrective action plan, please provide copies of the proposals submitted to airport owners where a Coordination Center is located, requesting access to closed-circuit television.

Recommendation #7: Provide all Coordination Centers with access to federal law enforcement data systems.

Management Response

The Department did not concur with Recommendation #7. TSA stated that access to criminal records is controlled by statute, regulations implemented by the Department of Justice, state laws, and policy. Therefore, TSA's ability to conduct a name-based criminal records check would depend on the reason for the search and type of activity taking place at a Coordination Center. TSA noted that, while expanded access to federal law enforcement data systems is an overall TSA goal, pushing access to federal law enforcement information sources to the Coordination Centers is not the most effective solution. The primary role of the Coordination Centers is to provide local support to TSA daily mission operations while monitoring transportation-related information sources within airports. Coordination Centers work in concert with TSA's Transportation Security Operations Center, which is charged with providing 24/7/365 coordination, communications, intelligence, and domain awareness for all DHS transportation-related security activities worldwide. When managing an incident requiring coordination with federal law enforcement or other specialized database checks, Coordination Centers are expected to contact the Transportation Security Operations Center to obtain this information. This ensures that TSA handles information in accordance with relevant criminal history record information based on law and policy.

OIG Analysis

TSA states that the primary role of the Coordination Centers is to provide local support to TSA daily mission operations while monitoring transportation-related information sources within airports. Coordination Centers play a critical role in information sharing on foreign nationals. However, without direct and real-time access to federal law enforcement data systems, the centers are hindered in gathering and disseminating information that may

adversely affect transportation modes. TSA's overall goal is to expand access to federal law enforcement data systems, but statutes and regulations restrict access to criminal records. To resolve this issue, we encourage TSA to request a permanent Coordination Centers liaison from CBP OFO to improve TSA's access to timely information on foreign nationals via federal law enforcement data systems when a need to know is established. Both CBP and TSA officials have stated that they would like TSA to use DHS systems, particularly TECS, to obtain and share information. This collaboration between CBP and TSA would further strengthen aviation security and expand local support within the airport environment, eliminate delayed responses in an emergency, and improve information sharing between the components.

Recommendation #8: Provide federal law enforcement agencies updated training or guidance on the operational capabilities the Air and Marine Operations Center offers to support border security initiatives.

Management Response

The Department concurred with Recommendation #8. CBP stated that a strategic goal of CBP's AMOC is to continue to strengthen interagency and component partnerships to maximize homeland security strategies. One objective of AMOC is to continue to promote its missions, capabilities, and operations across components and interagency organizations. AMOC hosts more than 2,500 visitors annually from various law enforcement agencies to which it provides information regarding AMOC capabilities. Training is accomplished at law enforcement conferences; intelligence meetings; dedicated training on air smuggling laws, authorities, and current indicators; as well as dedicated AMOC training held at the Federal Law Enforcement Training Center.

OIG Analysis

CBP's plans are responsive to the recommendation. Its efforts to inform partners about AMOC's domain awareness capabilities will lead to better cooperation and understanding of AMOC's role in border security. In the corrective action plan, please provide copies of meeting minutes, memorandums, outreach program agendas, invitations, training manuals, and other evidence to indicate that AMOC regularly meets with other components and partners at the state and local levels to promote its operational capabilities.

We initiated this review to assess how biometric and biographic information is shared among DHS components at the U.S. air, land, and sea ports of entry, and land and maritime borders, focusing on—

- How components check and evaluate information when they make border determinations on foreign nationals who seek admission to the United States;
- The timeliness and thoroughness of information sharing;
- Interpersonal relationships among DHS components; and
- Infrastructure and resources challenges.

This is the second of three reports on information sharing among DHS components when they encounter a foreign national. The third report will examine information sharing on foreign nationals who are already inside the United States, both legally and illegally. Although our recommendations addressed resource challenges and professional relationships among DHS components, we limited the scope of this report to initiatives to screen foreign nationals at a U.S. port of entry or when they are apprehended between ports of entry. We did not review measures for U.S. citizens, except for programs that cover all travelers, and we did not evaluate cargo screening or agricultural inspection programs. We did not focus on privacy, civil rights, civil liberties, or redress aspects of the systems or processes. We wrote recommendations to improve communication and cooperation, policy and procedures, and timeliness and thoroughness of information sharing among DHS components.

We conducted fieldwork for this report from August to December 2010. We conducted 57 individual and group interviews with DHS personnel. We interviewed personnel from five DHS operational components—CBP, the Coast Guard, ICE, USCIS, and TSA—as well as personnel from the headquarters support office, Office of Policy. We reviewed documentation provided by DHS components and viewed many data systems demonstrations.

We conducted site visits to the following DHS offices:

During our field visits, our inspectors observed—

- CBP OFO's primary and secondary inspections at various land, sea, and air port of entry
- CBP OFO's Passenger Analysis Units at air ports of entry
- U.S. Border Patrol's operations
- CBP Air and Marine Operations Center
- CBP outbound passenger screening procedures
- The Coast Guard Vessel Screening program and Joint Harbor Operations Centers
- ICE ERO detainee intake procedures
- TSA's Operation Playbook exercises

We also conducted interviews with—

- USCIS Asylum Officers responsible for credible and reasonable fear processing
- CBP Air and Marine agents
- ICE HSI agents

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 FOR: Charles K. Edwards
Acting Inspector General

FROM: David Heyman
Assistant Secretary for Policy

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

Thank you for the opportunity to review and respond to the Office of Inspector General's (OIG) Draft Report entitled, "Information Sharing on Foreign Nationals: Border Security," (OIG-09-132a-ISP-DHS, Phase II). This memorandum is in response to your request that the Department of Homeland Security (DHS) Office of Policy (PLCY), in coordination with Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), and United States Citizenship and Immigration Service (USCIS) respond to the recommendations contained in the report.

This draft report provides analysis on information sharing among DHS components with border security missions and evaluates the timeliness and quality of information shared through DHS data systems and through communication among DHS component agencies. It also discusses how interagency working relationships affect operations to screen and process foreign nationals.

OIG acknowledges in the report that DHS has invested considerable resources to improve staffing and infrastructure, such as software to consolidate data systems. However, the OIG states that there is more work to be done in the area or resource allocation and prioritization in order to further improve upon information sharing.

The Department generally concurs with five of the eight recommendations and appreciates the opportunity to comment on the draft report. Listed below are the eight OIG recommendations and corresponding DHS responses.

Recommendation #1: Fully terminate the National Security Entry-Exit Registration System and reinstate the prior provisions.

DHS Response: Non-Concur. The National Security Entry-Exit Registration System (NSEERS) regulations were promulgated in the immediate aftermath of 9/11 by a formal rulemaking under the Administrative Procedure Act. This rulemaking was an exercise of the Attorney General's authority to require aliens to register in order to better protect the United States. From March 1, 2002 through April 28, 2011, the Secretary of Homeland Security exercised this authority primarily through country designations requiring information collection

by the NSEERS program. The Secretary, in her sole discretion, chose to end the collection of information under country designations by means of an April 28, 2011, Federal Register Notice.

The Secretary's authority, as exercised under the NSEERS regulations, is broader than the information collection program based on country designation described in the Office of Inspector General's draft report. The Secretary has chosen to retain this regulatory framework to enable prompt action to require registration of a category or categories of aliens, if necessary, through rapid publication of a Federal Register Notice. The retention of this regulatory framework has no direct cost to the Department while a formal rulemaking to rescind the regulations would be costly and time consuming now, with the possibility that another costly and time consuming rulemaking would be necessary if specific registration was needed in the future. Indeed, in light of the legally required time to promulgate new regulations, it might not be possible to reestablish a categorical registration regime in time fully to protect the United States from a future, perhaps imminent threat. The regulation is being kept in place to ensure that the Secretary retains a legal discretionary regulatory framework in case it is needed in the future.

Recommendation #2: Collaborate with commercial airlines and develop solutions to reduce the incidence of duplicate flight manifests.

DHS Response: Concur. CBP believes that it has successfully implemented this recommendation and respectfully requests closure. Duplicate manifests are largely a result of the implementation of the TSA Secure Flight program. CBP has taken several steps to resolve the issues identified in this finding. As part of the DHS One Solution process, carriers transmit data to the DHS for both the CBP Advance Passenger Information System (APIS) and TSA Secure Flight programs. Secure Flight and APIS have different time requirements that often result in carriers providing manifest information multiple times from multiple systems for the same passenger.

In 2009, CBP began receiving passenger transmissions 72 hours prior to departure due to TSA's Secure Flight requirement, as well as completed and validated APIS transmissions. CBP immediately identified the large numbers of duplicate records since several carriers' systems did not have the technical ability to link 72-hour data with the completed APIS manifest submissions for the same passenger and assisted the carriers with technical solutions to the duplication issue. CBP implemented the Flight Close Out message process whereby carriers are required to identify who is on the aircraft. The Flight Close Out message reconciles the APIS records transmitted and identifies those passengers on board the aircraft from those that were transmitted but did not board the aircraft. This assists the officers in identifying which set of biographic information should be used in the screening process.

CBP has implemented changes to enhance the officer's ability to screen the correct manifest entry by identifying which set of information represents the traveler on board the aircraft; corrected the system error that prevented lookouts from displaying when duplicate manifest entries existed; and removed those records identified as not on board from primary processing to ensure officers are processing only the screened passenger data.

Recommendation #3: Establish department-level oversight to address Customs and Border Protection, Office of Border Patrol, and Immigration and Customs Enforcement Homeland Security Investigations operational challenges.

DHS Response: Concur. The Department continues to exercise its oversight and coordination responsibility. This capability is presently carried out through a variety of fora and is becoming more robust as the Department matures. Of particular note, given the focus of this report, is the Information Sharing Governance Board (ISGB), which is a principal-level, Department-led coordination body. The ISGB serves as the executive-level decision-making body for all DHS information sharing matters. Chaired by the Under Secretary for Intelligence & Analysis, the ISGB includes DHS operational and headquarters elements. The ISGB meets quarterly to provide support for the Department's information sharing programs and participation in the National Information Sharing Environment (ISE). Furthermore, DHS selected a Senior Executive Level Manager to serve as the Department's Law Enforcement Information Sharing Initiative (LEISI) Executive Director. This selection demonstrated the importance and priority that DHS has placed on sharing of law enforcement information through various programs such as the LEIS Service, which has to date, been deployed in multiple locations in the United States and greatly enhances law enforcement sharing within all levels and entities of US and tribal law enforcement. DHS LEISI continues to be an active advocate for law enforcement information sharing within DHS and its components, and repeatedly coordinates throughout the law enforcement community to improve the understanding of information needs. Additionally, DHS LEISI provides important leadership in resolving policy issues that may inhibit law enforcement information sharing and strives to develop approaches to overcome traditional barriers to information sharing. Additionally, and with specific regard to the U.S. Northern Border, DHS will soon release its Northern Border Strategy and the Office of National Drug Control Policy (ONDCP) will soon release the Interagency Northern Border Counter Narcotics Strategy. These strategies will lay the groundwork, which will allow DHS to better coordinate internally between CBP, ICE, and components; to identify both gaps and duplication; and to achieve effective and efficient northern border management. Through these and other similar activities, the Department is strengthening its oversight and coordination responsibilities.

With respect to the particular coordination issues raised, CBP and ICE will be taking the following corrective actions:

- U.S. Border Patrol and ICE Homeland Security Investigations (HSI) will regularly collaborate on quarterly joint intelligence threat assessments by geographic area to identify and prioritize specific threats common to both agencies.

- U.S. Border Patrol and ICE HSI will jointly plan operations and allocate resources to disrupt and mitigate priority threats identified in joint assessments.

- U.S. Border Patrol and ICE HSI will formalize a joint information and data sharing protocol, to include shared access to agency-specific data systems.

- U.S. Border Patrol will cooperate to identify specific objectives within Customs and Border Protection to bridge the identified gap between intelligence gathering and operations requiring short-term investigations. This will allow for the efficient utilization

of organic resources within Customs and Border Protection, while allowing Homeland Security Investigations to focus more of their resources on their mission priorities.

Recommendation #4: Establish timeliness criteria for completing reasonable fear cases.

DHS Response: Concur. For Fiscal Year 2011, the Asylum Division in USCIS established a key initiative, "*Establish a timeliness standard for reasonable fear cases*." Pursuant to this key initiative, Headquarters Asylum (HQASM) consulted with the Asylum Offices and subsequently developed and executed a survey gathering descriptions of processing problems causing delays, the lengths, sources, and frequencies of those delays and other feedback. HQASM analyzed reports of case processing data from the Asylum Pre-Screening System (APSS) to assist in determining standards and benchmarks for the reasonable fear process.

In accordance with the Fiscal Year 2011 key initiatives, HQASM established the performance measure that 85% of reasonable fear cases must be completed within 90 days. This will measure the time between the referral date of the case from U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal (ERO) to the Asylum Office ("Clock-in Date" in APSS) to case completion ("Decision Served" or "Close Effective" in APSS). An additional performance measure is that 95% of pending reasonable fear cases must not be pending for more than 150 days. HQASM will require that Asylum Offices submit written justification for every case older than 150 days and provide updates every 30 days thereafter regarding progress on resolving the issues preventing decision issuance. Further analysis will assist in developing additional internal benchmarks.

Additionally, during the third quarter of Fiscal Year 2011, in recognition of the headquarters review delays referenced in the OIG report, HQASM detailed field supervisory asylum officers and quality assurance/training asylum officers to assist with the review of reasonable fear cases.

For Fiscal Year 2012, HQASM has developed two key initiatives. The first initiative is to implement Refugee, Asylum and International Operations Directorate Quality Assurance (RAIO QA) review of Reasonable Fear determinations and pilot RAIO QA review of Credible Fear determinations. The second initiative for Fiscal Year 2012 consists of implementing the two processing standards for reasonable fear established in Fiscal Year 2011, as described above. Both of these new measures will be promulgated at the beginning of Fiscal Year 2012 through the annual memorandum to Asylum Office Directors outlining each Asylum Office's performance objectives for the fiscal year. In addition, HQASM plans to modify APSS, reasonable fear procedures, and weekly reports in order to further standardize APSS data-entry and to assist Asylum Offices with the timely completion of reasonable fear determinations.

Recommendation #5: Record in the Asylum Pre-Screening System database the date when each reasonable fear case is returned to U.S. Immigration and Customs Enforcement jurisdiction.

DHS Response: Non-concur. As discussed between USCIS Asylum Division and the Office of Inspector General (OIG), this recommendation was based on a perceived data deficiency in the Asylum Pre-Screening System (APSS) database resulting in the Asylum Division being unable to assess reasonable fear case completions. The OIG recommendation was for the Asylum

Division to record when each reasonable fear case is returned to ICE jurisdiction as indication of case completion.

After the exit conference, the OIG requested that USCIS provide additional information on the APSS database to clarify the current data entry procedure in APSS and how the Asylum Division assesses case completions for reasonable fear. The Asylum Division clarified that the APSS data field ("Decision Served") is used to assess timeliness and completion for reasonable fear cases. The "Decision Served" date encompasses the change of jurisdiction from USCIS Asylum to the Department of Justice - Executive Office for Immigration Review (DOJ/EOIR) and to ICE.

Since the Asylum Division does have a way to record and assess reasonable fear timeliness and completions, OIG indicated that this recommendation would be closed for cause upon issuance of the final report. USCIS agrees with OIG that this recommendation should be closed.

Recommendation #6: Provide all Coordination Centers with live video feeds from security cameras in the airport terminals.

DHS Response: Concur. The Coordination Center (CC) is the primary communication hub for all TSA activity within the FSD domain. The CC continuously monitors, coordinates, and communicates situational and domain awareness of multimodal transportation activities and acts as the primary information and reporting conduit for security related incidents and/or emergencies. The CC serves as the focal point for TSA steady state operations. When applicable, CCs will transition to an Incident Command System (ICS) focusing on Incident Management (IM) and/or Emergency Management (EM).

TSA recognizes that the TSA Coordination Centers can play an increasing role in information sharing on foreign nationals in the commercial airport environment. Currently, access to CCTV is coordinated on the local level through TSA, airport operator and other entities with a need to know. Access to CCTV is airport owned and often this effort is logistically challenging. Additionally, due to the variations of CCs infrastructure not all CCs are operationally set-up or located to receive CCTV. In order to fully maximize the Coordination Centers' one-stop shop of information for TSA and its federal, state, and local agency partners at the local level, TSA will consider the resources available and whether or not we are able to expand such access.

Recommendation #7: Provide all Coordination Centers (CC) with access to federal law enforcement data systems.

DHS Response: Non-concur. Access to criminal records is controlled by statute (The National Crime Prevention and Privacy Compact Act of 1998, 42 U.S.C. 14616), regulations implemented by the Department of Justice (28 CFR 20.33), State laws, and policy. Individuals engaged in certain criminal investigative activities may conduct name-based criminal record searches as necessary. However, certain other activities require the collection and submission of fingerprints and fees to the FBI in order to conduct a criminal records search. Thus, TSA's ability to conduct a name-based criminal records check would depend on the reason for the search and type of activity taking place at a CC.

While expanded access to Federal law enforcement data systems is an overall TSA goal, pushing access to federal law enforcement information sources to the Coordination Centers is not the most effective solution. The primary role of the CC is to provide local support to TSA daily mission operations while monitoring transportation-related information sources within an FSD domain. Coordination Centers facilitate the gathering, dissemination, communication, and reporting of information to the Transportation Security Operations Center (TSOC) on a 24/7 basis, conduct routine ongoing operations and provide an incident management communication and coordination framework for FSD initial-response actions.

The CCs work in concert with TSA's Transportation Security Operations Center (TSOC), which is charged with providing 24 hours a day, 7 days a week, 365 days a year coordination, communications, intelligence and domain awareness for all DHS transportation related security activities worldwide. When managing an incident requiring coordination with Federal law enforcement or other specialized database checks, CCs are expected to contact TSOC to obtain this information, consistent with TSA Operations Directives. This ensures TSA handles information in accordance with relevant criminal history record information law and policy.

Recommendation #8: Provide federal law enforcement agencies updated training or guidance on the operational capabilities the Air and Marine Operations Center offers to support border security initiatives.

DHS Response: Concur. CBP believes that its ongoing efforts meet the intent of this recommendation and respectfully requests closure of the recommendation. A strategic goal of CBP's Air and Marine Operations Center (AMOC) is to continue to strengthen interagency and component agency partnerships to maximize homeland security strategies. To help accomplish this, an objective of the AMOC is to continue to promote AMOC missions, capabilities, and operations across component and interagency organizations. AMOC intelligence and law enforcement teams, along with AMOC Ambassadors, continuously provide law enforcement agencies at the federal, state, and local levels with information on AMOC's capabilities. The AMOC hosts more than 2,500 visitors annually from various law enforcement agencies to which it provides information regarding AMOC capabilities. Training is accomplished at law enforcement conferences; intelligence meetings; dedicated training on air smuggling laws, authorities, and current indicators; as well as dedicated AMOC training held at the Federal Law Enforcement Training Center. AMOC will continue to be proactive in these outreach and training efforts.

Appendix C
DHS Border Security Data Systems

DHS INFORMATION SYSTEMS	
Owner	**Manages Information on Foreign Nationals (who may become citizens)**
US-VISIT	**ADIS**
➢	Arrival and Departure Information System
➢	Collects, matches, and reports on U.S. arrivals and departures
USCIS	**APSS**
➢	Asylum Pre-Screening System
➢	Tracks detained and nondetained credible fear and reasonable fear cases
USCIS	**CIS**
➢	Central Index System
➢	Documents the existence and status of most aliens known to DHS and the location of their alien files
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**
➢	Enforcement Case Tracking 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 and 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 U.S. citizens)
CBP	**APIS**
➢	Advance Passenger Information System
➢	Receives air and sea passenger manifests
The Coast Guard	**SANS**
➢	Ship Arrival Notification System
➢	Arrival/departure information from shipping agents from flagged vessels
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	**ICEPIC**
➢	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 U.S. citizens)
CBP	**TECS**
➢	TECS (not an acronym)
➢	Collects, analyzes, and shares law enforcement information

Source: Database documentation, demonstrations.

Appendix D
Asylum Pre-Screening Case Disposition

Asylum Pre-Screening Cases				
Current Status	**Credible Fear Cases**	**Percentage by Case Disposition**	**Reasonable Fear Cases**	**Percentage by Case Disposition**
Fear Established	19,030	67%	1,067	24%
Fear Not Established	4,792	17%	1,377	30%
Case Closed: Applicant Withdrew	4,345	15%	1,950	43%
Case Closed: Other	351	1%	86	2%
Case Pending	6	0%	52	1%
Total	**28,524**	**100%**	**4,532**	**100%**

Source: USCIS APSS data from June 1, 2005, to June 30, 2010.

Appendix E
Reasonable Fear Case Timeliness

Reasonable Fear Case Timeliness						
Reasonable Fear Cases Decision Stages	**Decisions with dates entered**	**Average days to complete stage**	**Number of decisions over 31 days**	**Percentage of decisions over 31 days**	**Number of decisions over 93 days**	**Percentage of decisions over 93 days**
Time Elapsed From the Date ICE or CBP Notified the Asylum Program of a Claim Until the Date an Initial Decision Was Made	2,436	33 days	847	35%	158	6%
Time Elapsed From the Date an Initial Decision Was Made Until the Date the Case Was Forwarded to Headquarters for Review	2,221	11 days	159	7%	25	1%
Time Elapsed From the Date the Case Was Forwarded to Headquarters Until the Date the Case Was Completed	1,850	29 days	682	37%	59	3%
Asylum Notification to Case Completion	1,904	72 days	1,486	78%	466	24%
Total Reasonable Fear Decisions (with and without start and end dates) = 2,444						
Total Reasonable Fear Decisions (including withdrawals) = 4,532						

Source: USCIS APSS data from June 1, 2005, to June 30, 2010

Appendix F
Major Contributors to this Report

Douglas Ellice, Chief Inspector
Lorraine Eide, Lead Inspector
Pharyn Smith, Senior Inspector
Michael Brooks, Inspector
LaDana Crowell, Inspector

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
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 e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

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

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

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

- E-mail us at DHSOIGHOTLINE@dhs.gov; or

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

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