Department of Homeland Security

Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security

OIG-13-09 (Revised)

December 2012

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

DEC 21 2012

MEMORANDUM FOR: The Honorable Janet Napolitano
Secretary

FROM: Charles K. Edwards
Acting Inspector General

SUBJECT: *Major Management Challenges Facing the Department of Homeland Security*

Attached for your information is our revised annual report, *Major Management Challenges Facing the Department of Homeland Security*, for inclusion in the Department of Homeland Security 2012 *Annual Financial Report*. The original report contained three incorrect footnotes; however we have corrected the three footnotes in the report. Please see the attached errata page for details.

Should you have any questions, please call me, or your staff may contact Anne L. Richards, Assistant Inspector General for Audits, at (202) 254-4100.

Attachment

Major Management Challenges Facing the Department of Homeland Security

The attached report presents our fiscal year 2012 assessment of the major management challenges facing the Department. As required by the *Reports Consolidation Act of 2000* (Public Law 106-531), we update our assessment of management challenges annually. As stipulated, the report summarizes what the Inspector General considers to be the most serious management and performance challenges facing the agency and briefly assesses the agency's progress in addressing those challenges.

As in previous years, the Department's major challenges are reported in broad areas. For better understanding of how these areas relate to the overall operations of the organization, they have been categorized into two main themes: Mission Areas and Accountability Issues.

Mission Areas

- Intelligence
- Transportation Security
- Border Security
- Infrastructure Protection
- Disaster Preparedness and Response

Accountability Issues

- Acquisition Management
- Financial Management
- IT Management
- Grants Management
- Employee Accountability and Integrity
- Cyber Security

Mission Areas

Securing the Nation against the entire range of threats that we face in an evolving landscape is a difficult task. The vision and purpose of the Department of Homeland Security (DHS) is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.[1] At its establishment in 2003, the Department faced the challenge of building a cohesive, effective, and efficient Department from 22 disparate agencies, while simultaneously performing the mission for which it was created. As a whole, DHS has made progress in coalescing into a more cohesive organization to address its key mission areas to secure our Nation's borders, increase our readiness, build capacity in the face of a terrorist threat or a natural disaster, and enhance security in our transportation systems and trade operations.

Intelligence

Overview

Intelligence is vital to DHS' framework for securing the Nation. The development, blending, analysis, and sharing of intelligence with appropriate Federal, State, local, tribal, and territorial officials, as well as with private sector partners, must be timely and well coordinated to effectively predict terrorist acts.

Department intelligence programs, projects, activities, and personnel, including the intelligence elements of seven key DHS components, as well as the Office of Intelligence and Analysis (I&A), make up the DHS Intelligence Enterprise. I&A is charged with ensuring that intelligence from the DHS Intelligence Enterprise is analyzed, fused, and coordinated to support the full range of DHS missions and functions, as well as the Department's external partners. The components, most of which predate the creation of the Department, have intelligence elements that provide support tailored to their specialized functions and contribute information and expertise in support of the Department's broader mission set.[2]

[1] http://www.dhs.gov/our-mission

[2] Statement for the Record of Caryn A. Wagner, Under Secretary and Chief Intelligence Officer, Office of Intelligence and Analysis, before the Subcommittee on Counterterrorism and Intelligence House Committee on Homeland Security, "The DHS Intelligence Enterprise - Past, Present, and Future," June 1, 2011.

Challenges

Improving and enhancing support to fusion centers remains a challenge for the Department. To promote greater information sharing and collaboration among Federal, State, and local intelligence and law enforcement entities, State and local authorities established fusion centers throughout the country. A fusion center is a collaboration of two or more agencies to receive, gather, analyze, and disseminate information intending to detect, prevent, investigate, and respond to criminal or terrorist activity. The State and Local Program Office (SLPO), within the Office of Intelligence and Analysis, is responsible for coordinating and ensuring departmental support to the National Network of Fusion Centers.

In our fiscal year (FY) 2012 review, "*DHS' Efforts to Coordinate and Enhance Its Support and Information Sharing with Fusion Centers," w*e assessed: (1) whether the SLPO satisfies the intent of DHS' recommitment to the State, Local, and Regional Fusion Center Initiative; (2) whether planned SLPO efforts will ensure coordinated support of DHS and its components to provide needed information and resources to fusion centers; and (3) if any functional or organizational challenges in DHS hinder its successful support of fusion centers.

Accomplishments

DHS indicated that it has taken significant steps to improve the integration and coordination of intelligence products and processes across the Department. An enhanced analytic plan developed by I&A links data from disparate sources to help identify unattributed cyber intrusions threatening Federal and private sector networks. We determined that since July 2009, the SLPO has increased field support to fusion centers, worked to improve fusion center capabilities, and engaged DHS components. Efforts to develop a department-wide fusion center support strategy are ongoing, but improvements are needed to enhance the I&A's field deployments and DHS component support.[3]

[3] DHS-OIG, *DHS' Efforts to Coordinate and Enhance Its Support and Information Sharing with Fusion Centers (*OIG-12-10, November 2011).

Transportation Security

Overview

The Transportation Security Administration (TSA) is responsible for protecting the transportation system and ensuring the freedom of movement for people and commerce. The Nation's economy depends upon secure, yet efficient transportation security measures. Airport security includes the use of various technologies to screen passengers and their baggage for weapons, explosives, and other prohibited items, as well as to prevent unauthorized access to secured airport areas. As part of its responsibility, TSA is required to assess and test airport security measures on an ongoing basis to ensure compliance with policies and procedures and prevent security breaches.

Challenges

In spite of TSA's efforts, it continues to face challenges in passenger and baggage screening, airport security, the Secure Flight Program, airport badging, passenger air cargo security, training, as well as in providing oversight for the security of all modes of transportation including rail and mass transit.

Aviation

In regard to passenger and baggage screening, the *Aviation and Transportation Security Act* requires TSA to prescribe requirements for screening or inspecting all passengers, goods, and property before entry into secured areas of an airport. [4]

In its review of airport security, DHS OIG conducted covert testing of airport access controls as well as passenger and baggage screening. [5] Although test results are classified, access control and checkpoint screening vulnerabilities were identified at the domestic airports tested. Although Transportation Security Officers (TSO) were ultimately responsible for not fully screening checked baggage, our audit identified additional improvements that TSA can make in the evaluation of new or changed procedures, and improvements in supervision of TSOs that could have mitigated the situation.

In FY 2012, a congressional request led to a review of TSA's policies and practices governing its use of full-body x-ray screening equipment (general-use backscatter units)

[4] Public Law 107-71, November 19, 2001.
[5] DHS-OIG, *(U) Covert Testing of Access Controls to Secured Airport Areas* (OIG-12-26, January 2012).

for airport security. Congressman Edward J. Markey was concerned about the safety of the doses of radiation emitted by the units. TSA began deploying general-use backscatter units in March 2010, with 247 units operating in 39 commercial airports around the country at the time of publication of the FY 2012 backscatter unit report. In the United States, an x-ray system is considered compliant with requirements for general-purpose security screening of humans if it complies with standards of the American National Standards Institute.

Independent radiation studies conducted by professional organizations concluded that radiation levels emitted from backscatter units were below the acceptable limits. TSA entered into interagency agreements for additional radiation safety surveys and dosimetry measurement of the dose of radiation emitted by a radiation-generating device monitoring studies to document radiation doses to agency personnel and individuals being screened. All studies concluded that the level of radiation emitted was below acceptable limits.

The Secure Flight Program was implemented in October 2008 in an effort to bolster the TSA security directives established after the terrorist attacks of September 11, 2001. Under this program, TSA receives specific passenger and non-traveler data from the airlines and matches it against the government's watch list. TSA then transmits a boarding pass, with results back to the aircraft operator, so a boarding pass can be issued.

TSA relies on designated airport operator employees to process the badging applications. A July 2011 audit report showed that individuals who pose a threat may obtain airport badges and gain access to secured airport areas.[6] We analyzed vetting data from airport badging offices and identified badge holder records with omissions or inaccuracies in security threat assessment status, birthdates, and birthplaces. These problems existed because TSA did not: (1) ensure that airport operators had quality assurance procedures for the badging application process; (2) ensure that airport operators provided training and tools to designated badge office employees; and (3) require Transportation Security Inspectors to verify the airport data during their reviews.

Through passenger air cargo security, approximately 7.6 million pounds of cargo are transported on passenger planes each day. The Code of Federal Regulations (49 CFR) requires that, with limited exceptions, passenger aircraft may only transport cargo originating from a shipper that is verifiably "known" either to the aircraft operator or to the indirect air carrier that has tendered the cargo to the aircraft operator. Through covert testing we identified vulnerabilities in cargo screening procedures employed by

[6] DHS-OIG, *TSA's Oversight of the Airport Badging Process Needs Improvement (Redacted)* (OIG-11-95, July 2011).

air carriers and cargo screening facilities to detect and prevent explosives from being shipped in air cargo transported on passenger aircraft.[7] Although TSA has taken steps to address air cargo security vulnerabilities, the agency did not have assurance that cargo screening methods always detected and prevented explosives from being shipped in air cargo transported on passenger aircraft.

We conducted a review to determine how TSA identifies, reports, tracks and mitigates security breaches at airports nationwide.[8] We determined that TSA does not have guidance for and oversight of the reporting process. This need for guidance resulted in the agency missing opportunities to strengthen airport security. TSA agreed with the recommendations in our report, and as a first step, is developing a standard definition of a security breach. In addition, TSA is also updating its airport performance metrics to track security breaches and airport checkpoint closures at the national, regional, and local levels.

Rail and Mass Transit

Passenger rail stations are attractive terrorist targets because of the large number of people in a concentrated area. Amtrak provides passenger rail service for nearly 27 million passengers every year, using approximately 22,000 miles of rail in 46 states and the District of Columbia. Although grant recipients, such as Amtrak, transit agencies, and State and local authorities, coordinated risk mitigation projects at high-risk rail stations, Amtrak did not always use grant funds to implement mitigation strategies at the highest risk rail stations, in terms of casualties and economic impact.[9] Amtrak did not mitigate critical vulnerabilities reported in risk assessments. These vulnerabilities remain because TSA: (1) did not require Amtrak to develop a corrective action plan addressing its highest ranked vulnerabilities; (2) approved Amtrak investment justifications for lower risk vulnerabilities; and (3) did not document roles and responsibilities for the grant award process.

Accomplishments

TSA has taken action as recommended by our audit and inspection work. For instance, the agency began developing detailed utilization reports to ensure that the AIT units

[7] DHS-OIG, *Evaluation of Screening of Air Cargo Transported on Passenger Aircraft* (OIG-10-119, September 2010).
[8] DHS-OIG, *Transportation Security Administration's Efforts To Identify and Track Security Breaches at Our Nation's Airports* (OIG-12-80, May 2012).
[9] DHS-OIG, *DHS Grants Used for Mitigating Risks to Amtrak Rail Stations (Redacted)* (OIG-11-93, June 2011).

deployed are being used efficiently. TSA has also developed more training for TSOs, which should help their performance.

Since the Secure Flight Program assumed responsibility for passenger prescreening, TSA has provided more consistent passenger prescreening. The program has a defined system and processes to conduct watch list matching. To ensure that aircraft operators follow established procedures, the Secure Flight Program monitors records and uses its discretion to forward issues for compliance investigation. The program also includes privacy safeguards to protect passenger personal data and sensitive watch list records and information. The Secure Flight Program focuses on addressing emerging threats through multiple initiatives.

TSA issued a management directive giving the Operational and Technical Training Division responsibility for overall management of the analysis, design, development, and implementation of TSO training programs.

To identify and track security breaches better, TSA is refining the definition of what constitutes such breaches and implementing a tool to provide more oversight in this area. In addition, TSA is also updating its airport performance metrics to track security breaches and airport checkpoint closures at the national, regional, and local levels.

TSA continues to work on improving operations, keeping us informed of the progress made in response to our work.

Border Security

Overview

Securing the Nation's borders from illegal entry of aliens and contraband, including terrorists and weapons of mass destruction, while welcoming all legitimate travelers and trade, continues to be a major challenge. DHS apprehends hundreds of thousands of people and seizes large volumes of illicit cargo entering the country illegally each year. United States Customs and Border Protection (CBP) is responsible for securing the Nation's borders at and between the ports of entry. Within CBP, the mission of the Office of Border Patrol helps secure 8,607 miles of international borders.

Challenges

Although CBP has made progress in securing our borders, it continues to face challenges in the areas of the Free and Secure Trade program (FAST), bonded facilities, unmanned aircraft systems, and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT).

FAST is a commercial clearance program for pre-enrolled commercial truck drivers entering the United States from Canada and Mexico designed to facilitate the free flow of trade. FAST allows for expedited processing of enrolled trusted travelers, including FAST drivers who fulfill certain eligibility requirements. However, FAST's eligibility processes do not ensure that only eligible drivers remain in the program. CBP is hampered in ensuring that Mexican citizens and residents in the program are low risk because Mexico does not share Southern border FAST information with the United States to assist in vetting and monitoring drivers' eligibility. Although renewal is required every 5 years, ineligible drivers may be actively enrolled in the program, exposing the agency to increased risk of compromised border security.[10]

CBP is responsible for cargo security, including the accountability of the transfer to and storage of cargo at privately owned and operated bonded facilities. Based on audited background checks at 41 bonded facilities at five seaports, CBP did not have effective management controls to ensure that bonded facility employees do not pose a security risk at these facilities. Additionally, CBP neither issued national requirements for background checks on employees of bonded facilities nor ensured that port directors had management controls over background checks at these facilities. As a result, background checks were inconsistent and often ineffective. This may put bonded facilities at greater risk for terrorist exploitation, smuggling, and internal conspiracies. CBP and United States Immigration and Customs Enforcement's (ICE's) Joint Fraud Investigative Strike Teams conducted unannounced investigations of bonded facilities resulting in the detention of more than 350 undocumented workers and workers with outstanding arrest warrants.[11]

Unmanned aircraft systems help secure the Nation's borders from illegal entry of aliens, including terrorists, and contraband, including weapons of mass destruction. These long-endurance, medium-altitude remotely piloted aircrafts provide reconnaissance, surveillance, targeting, and acquisition capabilities. CBP did not adequately plan resources needed to support its current unmanned aircraft inventory. Although CBP developed plans to use the unmanned aircraft's capabilities, its Concept of Operations planning document did not adequately address processes: (1) to ensure that required operational equipment was at each launch and recovery site; (2) for stakeholders to submit unmanned aircraft mission requests; (3) to determine how mission requests were prioritized; and (4) to be reimbursed for missions flown for stakeholders. CBP risks having substantially invested in a program that limits resources and its ability to achieve Office of Air and Marine mission goals.[12]

---

[10] DHS-OIG, *Free and Secure Trade Program-Continued Driver Eligibility* (OIG-12-84, May 2012).
[11] DHS-OIG, *CBP's Management Controls Over Bonded Facilities* (OIG-12-25, January 2012).
12 DHS-OIG, *CBP's Use of Unmanned Aircraft Systems in the Nation's Border Security* (OIG-12-85, May 2012).

CBP faces challenges in systematically identifying and flagging potential use of fraudulent biographic identities in its US-VISIT system.[13] An analysis of data showed 825,000 instances in which the same fingerprints were associated with different biographic data. These differences ranged from misspelled names and transposed birth dates to completely different names and birth dates. In some cases individuals may have supplied different names and dates of birth at ports of entry; in others individuals may have used different biographic identities at a port of entry after they had applied for a visa under a different name or been identified as a recidivist alien. Inaccurate and inconsistent information reduces the accuracy of US-VISIT data monitoring and impedes the ability to verify that individuals attempting to enter the United States are providing their true names and dates of birth.

Accomplishments

CBP indicated it continues to develop a streamlined and cost-effective process to be used by port offices when conducting background vetting of bonded facility applicants, officers and principals. This process will add significant oversight, tracking and reporting capabilities to the background vetting process and will allow CBP to determine the criminal history of any current or prospective bonded facility applicant. According to CBP officials, US-VISIT has programs to identify individuals who may have overstayed the condition of their visas and manually analyzes entry and exit data to associate fingerprints with biographic information. Stronger oversight of this program will keep better track of individuals entering the United States.

Infrastructure Protection

Overview

Protecting the Nation's critical physical and cyber infrastructure is crucial to the functioning of the American economy and our way of life. Critical infrastructure provides the means and mechanisms by which critical services are delivered to the American people; the avenues that enable people, goods, capital, and information to move across the country. The Department leads the effort, in collaboration with Federal, State, local, regional, and private sector partners, to enhance the protection and resilience of critical infrastructure. Ensuring the security of our critical infrastructure and key resources remains a great challenge.

[13] DHS-OIG, *US-VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities* (OIG-12-111, August 2012).

Challenges

Catastrophic failures in critical structures such as dams could affect more than 100,000 people and have economic consequences surpassing $10 billion. Yet, the Department could not ensure that risk assessments of dams were conducted or that security risks were identified and mitigated.[14] Specifically, the Department did not review all critical dam risk assessments conducted by other departments and agencies, did not conduct security reviews at 55 percent of critical dams, and did not ensure completion of corrective actions to mitigate risk were completed. Cooperation and collaboration with its security partners is essential to DHS' success in assessing risk and consequently, protecting critical infrastructure such as dams. The *National Infrastructure Protection Plan* prescribes a voluntary partnership between the government and the private sector to manage such risks. The Department does not have the authority to require dam owners to undergo security reviews or implement corrective actions.

DHS' Federal Protective Service (FPS) is responsible for the safety and security of more than 9,000 Federal facilities; the service employs 1,225 Federal staff members and uses 15,000 contracted security guards to carry out its mission. In August 2008, FPS funded a $21 million, 7-year contract to develop and maintain the Risk Assessment and Management Program (RAMP). RAMP was intended to assess and analyze risks to Federal facilities and recommend and track countermeasures, as well as manage post inspections, guard contracts, and guard certification compliance. However, in May 2011, FPS ceased development of RAMP because it was not cost effective and had not met its original goals. In July 2011, the Government Accountability Office (GAO) reported that RAMP's actual costs were more than three times the original $21 million development contract amount, the program was behind schedule, and the system could not be used as intended to complete security assessments or guard inspections. The contract was extended for 1 year to operate and maintain RAMP. Although FPS has stopped its development, the system is still being used to manage its guard force, and it contains historical data that FPS wants to retain and maintain. As of August 2012, FPS had determined its data needs and was working with the RAMP vendor to preserve historical documents and guard-related data.[15] DHS has completed data capture and decommissioned RAMP.

Additionally, according to an August 2012 GAO report, FPS has not effectively led the government facilities sector.[16] It has not obtained data on facilities or coordinated or assessed risk, all of which are key to risk management and safeguarding of critical

[14] DHS-OIG, *DHS Risk Assessment Efforts in the Dams Sector* (OIG-11-110, September 2011).
[15] DHS-OIG, *Federal Protective Service's Exercise of a Contract Option for the Risk Assessment and Management Program* (OIG-12-67, August 2012).
[16] GAO, *Critical Infrastructure: DHS Needs to Refocus its Efforts to Lead the Government Facilities Sector* (GAO-12-852, August 2012).

facilities. Furthermore, FPS has not built effective partnerships across different levels of government, needs a dedicated funding line for its activities in this area, and does not have an action plan for protecting facilities.

Accomplishments

To improve protection of the Dams Sector, DHS is nearing completion of its OIG-recommended assessment of the appropriateness of a legislative proposal to establish regulatory authority for the Dams Sector assets similar to that in the Chemical Sector. At the same time, the Department continues to make strides under the voluntary framework. This includes 100 percent completion of Infrastructure Protection assessments on privately-owned assets included on the FY 2011 Dams Sector critical assets list.

In regard to RAMP, DHS indicated it has minimized FPS costs and saved the government at least $13.2 million by stopping its development and paying the contractor only to operate and maintain the program. FPS also leveraged existing technology to develop the Modified Infrastructure Survey Tool nationwide. During the development, FPS continuously monitored the security posture of Federal facilities by responding to incidents, testing countermeasures, and conducting guard post inspections. Additionally, FPS has taken actions to enhance its coordination with sector-specific agencies for the government facilities sector. These include establishing new relationships with the State, Local, Tribal and Territorial Government Coordinating Council to ensure broader state and local participation in sector coordination procedures.

Disaster and Preparedness Response

Overview

The Federal Emergency Management Agency's (FEMA) task of coordinating emergency support following disasters has become more challenging as the number of events to which it responds has risen each year—from 25 to 70 since 1980. Additionally, FEMA spends an average of $4.3 billion each year in its response efforts. Although the agency has improved its disaster response and recovery, challenges remain.

Challenges

FEMA faces challenges in determining whether to declare events Federal disasters. FEMA uses preliminary disaster assessments to ascertain the impact and magnitude of damage from disasters and the resulting needs of individuals, businesses, the public sector, and the community. These assessments also help to determine whether events become federally declared disasters. In May 2012, we reported that, in deciding whether to declare an event a Federal disaster, FEMA used an outdated indicator that did not accurately measure the ability of State and local governments' to pay for damages.[17] If FEMA had updated the indicator, many recent disasters might not have met the financial conditions for Federal assistance.

In September 2012, GAO also noted that FEMA needed to improve the criteria it used to assess a jurisdiction's ability to recover from disasters.[18] In addition, GAO determined that FEMA had no specific criteria for assessing requests to raise the Federal share for emergency work to 100 percent. Finally, FEMA's administrative costs frequently exceeded its targets.

In evaluating FEMA's disaster recovery in Louisiana, we determined that only 6.3 percent of Katrina-related Public Assistance projects had been closed in the 72 months since the hurricane made landfall.[19] As of July 12, 2011, FEMA had obligated $10.2 billion in Public Assistance grants to support Louisiana's recovery from Hurricane Katrina. However, projects, especially time critical ones such as Debris Clearance and Emergency Work, were years past the closeout deadlines. FEMA, state officials, and subgrantees said the catastrophic damage was the major cause of delay in completing and closing out the Public Assistance projects. According to some officials, delays were also due to issues with the Federal Government's commitment to reimburse Louisiana for 100 percent of all Public Assistance project costs, FEMA's project procurement process, the agency's Public Assistance decision-making, and Louisiana staff resources. We recommended that FEMA develop project management policies, procedures, and timelines for Public Assistance projects that are 100 percent federally funded, coordinate with Louisiana and local governments to evaluate the status of Public Assistance projects, and expedite project closures.

FEMA must have a trained, effective disaster workforce to carry out its mission. As part of this effort, FEMA has a system to credential, or qualify and certify emergency

[17] DHS-OIG, *Opportunities to Improve FEMA's Public Assistance Preliminary Damage Assessment Process* (OIG-12-79, May 2012).
[18] GAO, *Federal Disaster Assistance: Improved Criteria Needed to Assess a Jurisdiction's Capability to Respond and Recover on Its Own* (GAO-12-838, September 2012).
[19] DHS-OIG, *Efforts to Expedite Disaster Recovery in Louisiana* (OIG-12-30, January 2012).

response providers through experience, training, and demonstrated performance. At the time of our June 2012 audit, however, FEMA had not completely implemented a credentialing program and had not identified an IT system to track the training, development, and deployment of disaster employees.[20] Additionally, the agency did not provide a detailed IT plan, documented costs, project schedule, and capability and/or performance requirements.

Our December 2011 audit report showed that some recipients of FEMA Public Assistance grants did not comply with a requirement to obtain and maintain insurance.[21] We also reported that States and FEMA could improve their monitoring and oversight to ensure recipients satisfy this requirement and do not receive financial aid for damages that are, or should be, covered by insurance. State and local governments are encouraged to obtain insurance to supplement or replace Federal Government assistance, but the Public Assistance program provides a disincentive to carry insurance. Although FEMA has been aware of this issue for more than 10 years, it has been slow to address it.

Providing the most efficient and cost-effective temporary post-disaster housing has been a major challenge for FEMA. The deployment of a large number of such housing after Hurricanes Katrina and Rita proved to be difficult. Later, some homes were found to contain high levels of formaldehyde, which led to health problems for disaster survivors. In the aftermath of these disasters, Congress provided FEMA funds to explore options for mitigating future disaster housing issues, including $400 million for an Alternative Housing Pilot Program and $1.4 million for the Disaster Housing Pilot Project.[22]

In the Alternative Housing Pilot Program, it was determined that the units developed were unlikely to match FEMA's needs for temporary housing. The Disaster Housing Pilot Project tested and evaluated 10 different types of housing units and provided options for more cost-effective, future housing, but FEMA put the project on hold because of inadequate funding. FEMA also terminated efforts to develop temporary housing units without indoor air quality issues, although in 2011, these efforts had resulted in model units with acceptable air quality levels. For future disasters, FEMA decided to house displaced disaster victims exclusively in mobile homes built to Department of Housing and Urban Development standards, which will eliminate many past problems. However, these units will likely cost more, are not suitable for flood plains, and will not fit on most urban home sites. The inability to use urban sites may hinder FEMA's capability to

[20] DHS-OIG, *FEMA's Progress in Implementing Employee Credentials* (OIG-12-89, June 2012).
[21] DHS-OIG, *FEMA's Process for Tracking Public Assistance Insurance Requirements* (OIG-12-18, December 2011).
[22] DHS-OIG, *Future Directions of FEMA's Temporary Housing Assistance Program* (OIG-12-20, December 2011).

respond quickly to disasters because alternative sites are limited, take more time to develop, and are frequently blocked by local communities. These sites are also much more expensive than private sites.

Accomplishments

FEMA continues to work on improving preliminary disaster assessments and recovery operations, keeping us informed of the progress made in response to our work. The Disaster Housing Pilot Project was created to evaluate innovative housing options by using them as student housing at a FEMA training facility. It is part of the effort to identify and evaluate alternative means of housing disaster survivors as directed by the Post-Katrina Act. Although the results of the evaluations are not yet complete, the project is providing a cost-effective means of identifying and testing alternative housing units.

FEMA is also pursuing data collection tools that will provide enhanced capabilities to perform Preliminary Damage Assessments (PDA) and record information in an efficient and consistent manner. FEMA is assessing the best available options for development of such a tool for PDAs, based on efforts to explore development of such a tool and in light of available technologies. Based on the findings of the assessment, FEMA plans to develop and implement the improved PDA data collection tool in FY13. This will improve PDA data collection, streamline the PDA process through use of an electronic system for data collection and reporting, and enhance the effectiveness of the PDA process.

According to FEMA, as of October 1, 2012, the FEMA Qualification System (FQS) became operational. FQS establishes the system for qualification and certification of the FEMA incident workforce through experience, training, and demonstrated performance. Throughout the year, milestones have been met to implement this critical program along with our other disaster workforce initiatives. While there will be continued development and expansion of the program FQS has been implemented for the entire incident management workforce.

FEMA is implementing other initiatives to improve disaster budgeting and program management once a declaration has been made that will enhance FEMA's ability to manage and budget for expenditures from the Disaster Relief Fund.

Accountability Issues

As the third largest agency in the Federal Government, DHS is responsible for managing a large workforce, and significant Federal resources. DHS is responsible for an annual budget of more than $59 billion, employs more than 225,000 employees and operates in more than 75 countries. At its establishment in 2003, DHS faced building a cohesive and efficient organization from 22 disparate agencies, while simultaneously performing the critical mission for which it was created. As a whole, DHS has made progress in coalescing into a more effective organization, establishing policies and procedures to set the groundwork for effective stewardship over its resources but challenges remain.

Acquisition Management

Overview

Effective oversight and management of acquisition processes is vital to DHS. At the time of our reporting in 2012, the Department had approximately 160 acquisition programs with estimated life cycle costs of more than $144 billion. DHS' acquisitions were numerous, varied, and complex, including everything from ships, aircraft, and vehicles to real estate, computer technology, and maintenance services.

Challenges

During FY 2012, both OIG and GAO conducted audits of acquisition management, examining individual acquisition programs and the underlying policies and procedures. We identified challenges the Department faces in the Secure Border Initiative. For example, along the southwest border, CBP has spent $1.2 billion to construct physical barriers as part of the Secure Border Initiative. As part of that effort, CBP did not effectively manage the purchase and storage of steel for fence construction, which cost about $310 million. It purchased steel before legally acquiring land or meeting international treaty obligations. In addition, CBP did not provide effective contract oversight, including not paying invoices on time and not reviewing the contractor's selection of a higher-priced subcontractor. As a result of these issues, CBP purchased more steel than needed, incurred additional storage costs, paid interest on late

payments, and approved a higher-priced subcontractor, resulting in expenditures of nearly $69 million that could have been put to better use.[23]

A November 2011 GAO review of the subsequent southwest border strategy, the Arizona Border Surveillance Technology Plan, showed that DHS did not document the analysis justifying the specific types, quantities, and deployment locations of border surveillance technologies proposed in the plan.[24] Without documentation DHS was hindered in its ability to verify that processes were followed, identify underlying analyses, assess the validity of the decisions made, and justify the requested funding.

Acquisition and resource management will continue to be a challenge for the United States Coast Guard (USCG) as it strengthens acquisition management capabilities and develops acquisition program baselines for each asset. According to GAO, the approved baselines for 10 of 16 programs did not reflect cost and schedule plans because programs breached the cost or schedule estimates in those baselines, changed in scope, or were not expected to receive funding to execute baselines as planned.[25] According to DHS, during 2012, two USCG program baselines were approved by DHS, two are pending DHS approval, and one is in USCG routing.

Since 2003, under a program to replace its aging HU-25 Falcon fleet, the USCG has taken delivery of 13 Ocean Sentry Maritime Patrol medium-range surveillance aircraft. In most instances, the USCG awarded the Ocean Sentry Maritime Patrol aircraft contracts effectively. However, it could have improved its oversight of the latest contract, awarded in July 2010 to the European Aeronautic Defense and Space Company North America for three aircraft valued at nearly $117 million. For this contract, the USCG was aware of conclusions by the Defense Contract Audit Agency regarding non-chargeable costs and noncompliance with the Federal Acquisition Regulation by the subcontractor, European Aeronautic Defense and Space Company/Construcciones Aeronáuticas Sociedad Anónima. The USCG was aware of the conclusions, and could have conducted additional follow up to ensure that the subcontractor had implemented recommendations made by the Defense Contract Audit Agency. The USCG also did not obtain sufficient support to ensure it excluded non-chargeable costs when awarding the latest contract.[26]

[23] DHS-OIG, *U.S. Customs and Border Protection's Management of the Purchase and Storage of Steel in Support of the Secure Border Initiative* (OIG-12-05, November 2011).
[24] GAO-OIG, *Arizona Border Surveillance Technology: More Information on Plans and Costs Is Needed Before Proceeding* (GAO-12-22, November 2012).
[25] GAO, *Coast Guard: Portfolio Management Approach Needed to Improve Major Acquisition Outcomes* (GAO-12-918, September 2011).
[26] DHS-OIG, *U.S. Coast Guard's Maritime Patrol Aircraft* (OIG-12-73, April 2012).

The Department continues to face challenges in integrating the 22 disparate legacy agencies and these challenges have a direct effect on acquisition management decisions. According to a September 2012 GAO report, DHS acquisition policy does not fully reflect several key portfolio management practices, such as allocating resources strategically, and DHS has not yet re-established an oversight board to manage its investment portfolio across the Department.[27] For example, there have been numerous efforts to find efficiencies between CBP's and USCG's aviation fleets. The Secretary's FY 2013 budget emphasized consolidating and streamlining systems and operations to ensure cost savings. In a March 2012 hearing, the Secretary highlighted efforts to increase the effectiveness of DHS' aviation assets through increased coordination and collaboration. In 2010, CBP and the USCG signed a joint strategy to unify their aviation management information systems. However, as of July 2012, CBP planned to acquire a new, separate IT system for its aircraft, which would continue past practices of obtaining disparate systems that did not share information with other components, including the USCG. We recommended that CBP terminate this planned acquisition and transition its aviation logistics and maintenance tracking to the USCG's system, in accordance with the Secretary's efficiency initiatives and the joint strategy. By transitioning to the USCG's system, CBP could improve the effectiveness of aviation management information tracking and save more than $7 million.[28]

Accomplishments

According to DHS, it has made progress in improving program governance, increasing insight into program performance, and building acquisition and program management capabilities. DHS has implemented requirements for tiered acquisition program reviews intended to increase its ability to identify and mitigate program risk. The Department has also implemented a Decision Support Tool to provide visibility into program health and has established Centers of Excellence to provide guidance.

In August, 2012, we reported that DHS was progressing toward the implementation of an information technology infrastructure at the St. Elizabeth's Campus in Washington, DC.[29] Specifically, DHS partnered with the General Services Administration to use its interagency information technology contracting vehicles. The General Services Administration also awarded a task order on behalf of DHS to acquire information technology resources for the Technology Integration Program.

[27] GAO, *DHS Requires More Disciplined Investment Management to Help Meet Mission Needs* (GAO-12-833, September 2012).
[28] DHS-OIG, *CBP Acquisition of Aviation Management Tracking System* (OIG-12-104, August 2012).
[29] DHS-OIG, *Adherence to Acquisition Management Policies Will Help Reduce Risks to the Technology Integration Program*, (OIG-12-107, August 2012).

The Department has created an Acquisition Workforce Development initiative to improve its acquisition workforce. This initiative includes expanding training opportunities and offering certification programs in Cost Estimating, Program Financial Management, Life Cycle Logistics, and Test and Evaluation and Systems Engineering. When the outcomes of this initiative are achieved the Department's acquisition workforce will be ready to acquire and sustain the systems and services necessary to secure the homeland, while ensuring that the Department and taxpayers received the best value for the expenditure of public resources.

Financial Management

Overview

The Federal Government has a fundamental responsibility to be an effective steward of taxpayer dollars. Sound financial practices and related management operations are critical to achieving the Department's mission and to providing reliable, timely financial information to support management decision-making throughout DHS. Congress and the public must be confident that DHS is properly managing its finances to minimize inefficient and wasteful spending, make informed decisions to manage government programs, and implement its policies.

Although DHS produced an auditable balance sheet and statement of custodial activity in FY 2011 and obtained a qualified opinion on those statements, challenges remain for the Department's financial management. Achieving a qualified opinion resulted from considerable effort by DHS employees, rather than through complete implementation of a reliable system of control over financial reporting. As a result of DHS obtaining a qualified opinion on its balance sheet and statement of custodial activity in FY 2011, the scope of the FY 2012 audit was increased to include statements of net cost, changes in net position, and combined statement of budgetary resources.

Challenges

Managerial Cost Accounting

The Department does not have the ability to provide timely cost information by major program, and by strategic and performance goals. The Department's financial management systems do not allow for the accumulation of costs, at the consolidated level, by major program, nor allow for the accumulation of costs by responsibility segments directly aligned with the major goals and outputs described in each entity's strategic and performance plan. Further, the Department needs to develop a plan to

implement managerial cost accounting, including necessary information systems functionality. Currently, the Department must use manual data calls to collect cost information from the various components and compile consolidated data.

OIG conducted several audits during FY 2012 and identified a number of components that did not have the ability to provide various cost data when requested. For example:

- During the audit of TSA's Aviation Channeling Service Provider program (OIG 12-132-AUD-TSA) we learned that TSA did not track and report all project costs related to the program. According to TSA program officials, it was impossible to provide exact costs because the expenditures were not tracked in detail.
- During the audit examining CBP's acquisition and conversion of H-60 helicopters (OIG 12-102-AUD-CBP), CBP officials received high-level cost information from the U.S. Army, but it did not include the detail necessary to adequately oversee the CBP H-60 programs. For example, the Army conducted approximately 15,000 tests on CBP H-60 components, but CBP could not identify the tests that were completed or the specific costs. In addition, for each CBP H-60 helicopter, financial data from three sources listed a different total cost for each helicopter.
- During the audit of CBP's use of radiation portal monitors at seaports (OIG 12-033-AUD-CBP), we found instances in which the acquisition values for the monitors were incorrect and could not be supported.

Anti-Deficiency Act Violations

The Department continues to have challenges in complying with the Anti-Deficiency Act (ADA). As of September 30, 2012, the Department and its components reported five potential ADA violations in various stages of review, including one potential ADA violation identified in FY 2012, which the Department is currently investigating. The four other ADA violations involve: (1) expenses incurred before funds were committed or obligated; (2) pooled appropriations to fund shared services; (3) a contract awarded before funds had been re-apportioned; and (4) improper execution of the obligation and disbursement of funds to lease passenger vehicles.

Financial Statement Audit

The following five items show the status of DHS' effort to address internal control weaknesses in financial reporting. These were identified as material weaknesses in the FY 2011 independent audit of DHS' consolidated balance sheet and statement of custodial activity. All five material weaknesses remain in FY 2012.

Financial Reporting

Financial reporting presents financial data on an agency's financial position, its operating performance, and its flow of funds for an accounting period.

In FY 2011 the USCG, USCIS, and TSA contributed to the material weakness in this area. While some findings reported in FY 2011 were corrected, other findings at USCG and TSA remained in FY 2012. Also, in FY 2012, new financial reporting findings were identified at ICE.

As in the previous year, the auditors reported this year that the USCG does not have properly designed, implemented, and effective policies, procedures, processes, and controls surrounding its financial reporting process. The USCG uses three general ledgers, developed over a decade ago. This legacy system has severe functional limitations that contribute to its ability to address systemic internal control weaknesses in financial reporting, strengthen the control environment, and comply with relevant Federal financial system requirements and guidelines.

The auditors identified deficiencies that remain in some financial reporting processes at TSA. For example, there are weak or ineffective controls in some key financial reporting processes, of the management's quarterly review of the financial statements, and in supervisory reviews over journal vouchers. In addition, TSA has not fully engaged certain program and operational personnel and data into the financial reporting process and is not fully compliant with the United States Government Standard General Ledger requirements at the transaction level. In recent years, TSA implemented several new procedures and internal controls to correct known deficiencies, but some procedures still require modest improvements to fully consider all circumstances or potential errors. The control deficiencies contributed to substantive and classification errors reported in the financial statements and discovered during the audit.

During FY 2012, the auditors noted financial reporting control weaknesses at ICE, primarily resulting from expanded audit procedures for the full-scope financial statement audit. ICE has not fully developed sufficient policies, procedures, and internal controls for financial reporting. It also needs adequate resources to respond to audit inquiries promptly, accurately, and with the ability to identify potential technical accounting issues. ICE faces challenges in developing and maintaining adequate lines of communication within its Office of Financial Management and among its program offices. Communication between financial managers and personnel responsible for contributing to financial reports was not sufficient to consistently generate clear and usable information. In addition, ICE does not have sufficient coordination with IT

personnel, including contractors, who are responsible for generating certain financial reports.

Information Technology Controls and Financial Systems Functionality

IT general and application controls are essential to effective and reliable reports of financial and performance data.

During the FY 2011 financial statement audit, the independent auditor noted that the Department remediated 31 percent of the prior year IT findings. The most significant FY 2011 weaknesses include: (1) excessive unauthorized access to key DHS financial applications, resources, and facilities; (2) configuration management controls that are not fully defined, followed, or effective; (3) security management deficiencies in the certification and accreditation process and an ineffective program to enforce role-based security training and compliance; (4) contingency planning that lacked current, tested contingency plans developed to protect DHS resources and financial applications; and (5) improperly segregated duties for roles and responsibilities in financial systems. These deficiencies negatively affected the internal control over DHS' financial reporting and its operation and contributed to the FY 2011 financial management and reporting material weakness.

For FY 2012, DHS made some progress in correcting the IT general and application control weaknesses identified in FY 2011. DHS and its components remediated 46 percent of the prior year IT control weaknesses, with CBP, FEMA, and TSA making the most progress in remediation. Although CBP and FEMA made progress in correcting their prior year issues, in FY 2012, the most new issues were noted at these two components. New findings resulted primarily from new IT systems and business processes that came within the scope of the FY 2012 financial statement audit and that were noted at all DHS components.

The auditors noted many cases in which financial system functionality inhibits DHS' ability to implement and maintain internal controls, notably IT application controls supporting financial data processing and reporting. As a result, ongoing financial system functionality limitations are contributing to the Department's challenge to address systemic internal control weaknesses and strengthen the overall control environment.

In FY 2012, five IT control weaknesses remained and presented risks to the confidentiality, integrity, and availability of DHS' financial data: (1) access controls; (2) configuration management; (3) security management; (4) contingency planning; and (5) segregation of duties.

Property, Plant and Equipment

DHS capital assets and supplies consist of items such as property, plant, and equipment (PP&E) operating materials, as well as supplies, including boats and vessels at the USCG, passenger and baggage screening equipment at TSA, and stockpiles of inventory to be used for disaster relief at FEMA. The USCG maintains approximately 50 percent of all DHS PP&E.

During FY 2011, TSA, the USCG, CBP, and the Management Directorate contributed to a departmental material weakness in PP&E. During FY 2012, TSA and Management Directorate substantially completed corrective actions in PP&E accounting processes. In FY 2012, the USCG continued to remediate PP&E process and control deficiencies, specifically those associated with land, buildings and other structures, vessels, small boats, aircraft, and construction in process. However, remediation efforts were not fully completed in FY 2012. The USCG had difficulty establishing its opening PP&E balances and accounting for leases, primarily because of poorly designed policies, procedures, and processes implemented more than a decade ago, combined with ineffective internal controls and IT system functionality difficulties.

As in prior years, CBP has not fully implemented policies and procedures, or does not have sufficient oversight of its adherence to policies and procedures, to ensure that all PP&E transactions are recorded promptly and accurately, or to ensure that all assets are recorded and properly valued in the general ledger. Further in FY 2012, ICE did not have adequate processes and controls in place to identify internal-use software projects that should be considered for capitalization.

Environmental and Other Liabilities

Liabilities are the probable and measurable future outflow or other sacrifice of resources resulting from past transactions or events. The internal control weaknesses reported in this area are related to various liabilities, including environmental, accounts payable, legal, and accrued payroll and benefits.

The USCG's environmental liabilities represent approximately $500 million or 75 percent of total DHS environmental liabilities. The USCG completed the final phases of a multi-year remediation plan to address process and control deficiencies related to environmental liabilities later in FY 2012. However, the USCG did not implement effective controls to ensure the completeness and accuracy of all underlying data components used to calculate environmental liability balances. Further, the USCG did not have documented policies and procedures to update, maintain, and review schedules to track environmental liabilities (e.g., Formerly Used Defense Sites) for which it was not primarily responsible at the Headquarters level. Additionally, the USCG did not effectively implement existing policies and procedures to validate the prior year accounts payable estimate.

Budgetary Accounting

Budgetary accounts are general ledger accounts for recording transactions related to the receipt, obligation, and disbursement of appropriations and other authorities to obligate and spend agency resources. DHS has numerous sources and types of budget authority, including annual, multi-year, no-year, and permanent and indefinite appropriations, as well as several revolving, special, and trust funds. Timely and accurate accounting for budgetary transactions is essential to managing Department funds and preventing overspending.

The USCG implemented corrective actions plans over various budgetary accounting processes in FY 2012; however, some control deficiencies reported in FY 2011 remain, and new deficiencies were identified. Although FEMA also continued to improve its processes and internal controls over the obligation and monitoring process, some control deficiencies remain.

As the financial service reporting provider, ICE is responsible for recording budgetary transactions and administers budgetary processes across different types of funds at the National Protection and Programs Directorate, Science and Technology Directorate, Management Directorate, and Office of Health Affairs. In FY 2011, ICE identified and began remediating deficiencies in the financial management system that impact accounting transactions such as positing logic related to adjustments of prior year unpaid, undelivered orders. In FY 2012, ICE continued to address these issues with certain types of obligations.

Accomplishments

The Department continues to work on improving financial reporting. In FY 2012, DHS received a qualified opinion on its financial statements. Improvements were seen at various components. For example, USCIS corrected control deficiencies in financial reporting that contributed to the overall material weakness. Likewise, TSA made significant progress in addressing PP&E, removing its contribution to the Department's material weakness. Further, the USCG continued to make financial reporting improvements in FY 2012 by completing its planned corrective actions over selected internal control deficiencies. These remediation efforts allowed management to make new assertions in FY 2012 related to the auditability of its financial statement balances. In addition, management was able to provide a qualified assurance of internal control over financial reporting in FY 2012.

According to DHS' Office of Financial Management, there is improved access to and better quality of financial management information. The Department has implemented business intelligence tools to help organize, store, and analyze data more efficiently. According to the office, the Department can now take information from individual budgets and display it for the enterprise, allowing views of DHS' budget allocation by mission area. Additionally, the Department is developing management tools (Decision Support Tool) to help compile department-wide program cost information. The Decision Support Tool should provide a central dashboard to assess and track the health of acquisition projects, programs, and portfolios by showing key indicators of program health, such as cost, funding, and schedule.

IT Management

Overview

As technology constantly evolves, the protection of the Department's IT infrastructure becomes increasingly more important. The Department's Chief Information Officer (CIO) has taken steps to mature IT management functions, improve IT governance, and integrate IT infrastructure. Specifically, at the Department level, the CIO has increased IT governance oversight and authority by reviewing component IT programs and acquisitions. Although the Department's documented processes were still draft, these steps have enabled the CIO to make strategic recommendations to reduce costs and duplication through activities such as infrastructure integration, as well as data center and network consolidation.

Challenges

Several DHS components continue to face IT management challenges. For example, in a November 2011 audit, we reported that USCIS delayed implementing its transformation program because of changes in the deployment strategy and system requirements that were insufficiently defined prior to selecting the IT system solution.[30] Other challenges, such as the governance structure, further delayed the program. As a result, USCIS continued to rely on paper-based processes to support its mission, which made it difficult for the component to process immigration benefits efficiently, combat identity fraud, and provide other government agencies with information to identify criminals and possible terrorists quickly. USCIS took steps to address some of these challenges by moving to an agile development approach, instead of a "waterfall" process. This change

[30] DHS-OIG, *U.S. Citizenship and Immigration Services' Progress in Transformation* (OIG-12-12, November 2011).

improved program monitoring and governance and increased the focus on staffing issues.

According to a June 2012 audit, CBP needs to address systems availability challenges, due in part to an aging IT infrastructure.[31] Limited interoperability and functionality of the technology infrastructure made it difficult to fully support CBP mission operations. As a result, CBP employees chose to use alternative solutions, which may have hindered CBP's ability to accomplish its mission and ensure officer safety.

DHS has matured key information IT functions, such as portfolio management. However, in May 2012, we reported that recruiting people with the necessary skills to perform certain management functions remains a challenge. Also, DHS needs to improve its budget review process so that the CIO can identify and resolve issues before components finalize their IT investments.[32] In addition, GAO reported in July 2012 that DHS had a vision for its new IT governance process, which included a tiered oversight structure with distinct roles and responsibilities throughout the Department. However, DHS' IT governance policies and procedures were not finalized, which meant less assurance that its new IT governance would consistently support best practices and address previously identified weaknesses in investment management.[33]

CBP needs to improve its compliance with Federal privacy regulations. It also needs to establish an Office of Privacy with appropriate resources and staffing. Although DHS has a directive to ensure compliance with all privacy policies and procedures issued by the Chief Privacy Officer, an April 2012 audit disclosed that CBP made limited progress toward instilling a culture of privacy that protects sensitive personally identifiable information.[34] Without a component-wide approach that minimizes the collection of employee Social Security numbers, privacy incidents involving these numbers will continue to occur.

Accomplishments

The Department has created initiatives to improve IT Program Governance and Information Security. These programs are designed to prioritize programs to meet Department business needs, eliminate duplicate functions and systems, increase program accountability and strengthen internal controls.[35] Progress has been made to

[31] DHS-OIG, *CBP Information Technology Management: Strengths and Challenges* (OIG-12-95, June 2012).
[32] DHS-OIG, *DHS Information Technology Management Has Improved, But Challenges Remain* (OIG-12-82, May 2012).
[33] GAO, *DHS Needs to Further Define and Implement Its New Governance Process* (GAO-12-818, July 2012).
[34] DHS-OIG, *U.S. Customs and Border Protection Privacy Stewardship* (OIG-12-78, April 2012).
[35] DHS, *Integrated Strategy for High Risk Management: Implementation and Transformation* (June 2012).

meet the goals of these initiatives and once fully achieved, the Department will have increased accountability for its information technology programs.

According to DHS, the CIO has created performance measures to help establish accountability and determine progress and accomplishments in IT Program Governance. For example, one measure is the number of IT segments covered by portfolio governance. Since IT segments represent a subset of the Department's mission and a business portfolio, this measure has resulted in an increase in the number of IT functions that have governance in place. In the beginning of FY 2012, only 5 of 30 IT segments were covered by portfolio governance. By the end of FY 2012, the Office of the CIO achieved its target to attain portfolio governance for 10 of 30 (33 percent) IT segments. By the end of FY 2013, the office will capture an additional 5 segments to reach its goal of 50 percent (15 of 30). By FY 2016, the goal is to have all 30 functional areas with IT governance.

Grants Management

Overview

More than $35 billion in homeland security grants have been provided over the past 10 years to States, territories, local, and tribal governments to enhance capabilities to plan, prepare for, prevent, respond to, and recover from natural disasters, acts of terrorism, and other manmade disasters. In grants management, FEMA is challenged to ensure the grants process is transparent, efficient, and effective. FEMA must also provide oversight to a large number of geographically dispersed grant recipients to ensure Federal funds are used for their intended purposes.

Challenges

FEMA can improve its efforts in strategic planning, performance measurement, oversight, and sustainment, including tracking States' milestones and accomplishments for homeland security grant-funded programs. FEMA needs to improve its strategic management guidance for State Homeland Security Grants. In our most recent *Annual Report to Congress*, we summarized State Homeland Security strategies and identified deficiencies related to measurable goals and objectives. Although current guidance for State Homeland Security strategies encourage revisions every 2 years, such revisions are not required. Additionally, we identified State Homeland Security strategies that do not have goals and objectives that are specific, measurable, achievable, results-oriented, and time-limited. Without a measurable goal or objective, or a process to gather results oriented data, States may not be assured that their preparedness and response

capabilities are effective. States are also less capable of determining progress toward goals and objectives when making funding and management decisions.

FEMA has not provided sufficient guidance on establishing metrics and measuring performance. Our audits show that States continue to need the proper guidance and documentation to ensure accuracy or track milestones. Providing guidance on the appropriate metrics and requiring documentation of those metrics would help States understand the effectiveness of each grant program.

FEMA also needs to strengthen its guidance on reporting progress in achieving milestones as part of the States' annual program justifications. We determined that States' milestones for these continuing investment programs could not be compared to those in previous years' applications. Additionally, the status of the previous year milestones was not always included in applications. Because of these weaknesses, FEMA could not determine, from the annual application process, whether a capability had been achieved, what progress had been made, or how much additional funding was needed to complete individually justified programs. Without this information, FEMA could not be assured it made sound investment decisions.

Because of insufficient information on milestones and program accomplishments, FEMA annually awarded Homeland Security Grant Program funds to States for ongoing programs without knowing the accomplishments from prior years' funding or the extent to which additional funds were needed to achieve certain capabilities. Tracking accomplishments and milestones are critical to making prudent management decisions because of the changes that can occur between years or during a grant's period of performance.

FEMA needs to improve its oversight to ensure States are meeting their reporting obligations in a timely manner so that the agency has the information it needs to make program decisions and oversee program achievements. Improved oversight will also ensure that States are complying with Federal regulations on procurements and safeguarding of assets acquired with Federal funds. In our annual audits of the State Homeland Security Program, we repeatedly identified weaknesses in the States' oversight of grant activities. Those weaknesses include inaccuracies and untimely submissions of financial status reports; untimely allocation and obligation of grant funds; and not following Federal procurement, property, and inventory requirements.

Delays in the submission of Financial Status Reports may have hampered FEMA's ability to monitor program expenditures effectively and efficiently. They may also have prevented the States from drawing down funds in a timely manner and ultimately affected the functioning of the program. Delays also prevented the timely delivery of plans, equipment, exercises, and training for first responders.

In our audits in FYs 2011 and 2012, we noticed an emerging trend with issues related to program sustainment. States did not prepare contingency plans addressing potential funding shortfalls when DHS grant funding was significantly reduced or eliminated. In an era of growing budget constraints it is important to use resources for projects that can be sustained. FEMA addressed this issue in its FY 2012 grant guidance by focusing on sustainment rather than new projects.

Accomplishments

Although significant issues in grants management remain, progress has been made. In most instances, audited States efficiently and effectively fulfilled grant requirements, distributed grant funds, and ensured available funds were used. The States also continued to use reasonable methodologies to assess threats, vulnerabilities, capabilities, and needs, as well as allocate funds accordingly. Our audits have identified several effective tools and practices used by some States that could benefit all States; FEMA and the States also willingly shared information. FEMA has been responsive to our recommendations and the agency is taking action to implement those recommendations. At the Headquarters level, DHS is establishing a governance body that will determine high-risk areas such as those cited above, develop strategies to mitigate those risks and employ standardized formats, templates, and processes to ensure consistent financial assistance activities throughout DHS. Some of these standardized templates and processes are already in place.

Employee Accountability and Integrity

Overview

The smuggling of people and goods across the Nation's borders is a large scale business dominated by organized criminal enterprises. The Mexican drug cartels today are more sophisticated and dangerous than any other organized criminal groups in our law enforcement experience. Drug trafficking organizations are becoming increasingly more involved in systematic corruption of DHS employees to further alien and drug smuggling. The obvious targets of corruption are front line Border Patrol Agents and CBP officers; less obvious are those employees who can provide access to sensitive law enforcement and intelligence information, allowing the cartels to track investigative activity or vet their members against law enforcement databases. Although the number of DHS employees implicated in such enterprises is very small — less than 1 percent — the damage from even one corrupt employee represents a significant management challenge to the Department.

Border corruption affects national security. As demonstrated by investigations led by our investigators, border corruption may consist of cash bribes, sexual favors, or other gratuities in return for allowing contraband or undocumented aliens through primary inspection lanes; orchestrating illegal border crossings; leaking sensitive law enforcement information to persons under investigation; selling law enforcement intelligence to smugglers; and providing needed documents such as immigration papers. Corrupt employees most often are paid not to inspect, as opposed to allowing prohibited items, such as narcotics, to pass into the U.S. A corrupt DHS employee may accept a bribe for allowing what appears to be simply undocumented aliens into the U.S. while unwittingly helping terrorists enter the country. Likewise, what seems to be drug contraband could be weapons of mass destruction, such as chemical or biological weapons, or bomb-making material.

Challenges

We have seen a 95 percent increase in complaints against CBP employees alone since FY 2004 and a 25 percent increase from just fiscal year 2010 to 2011. In FY 2011, we received and disposed of 17,998 allegations involving all DHS employees. As of July 15, 2012, we had 1,591 open cases. Corruption-related allegations are a priority of the Office of Investigations, which opens 100 percent of all credible allegations of corruption it receives. The majority of both complaints received and investigations initiated by the OIG, however, are for allegations of other than corruption-related activity.

Since FY 2004, our investigations have resulted in 358 CBP related convictions and 166 ICE related convictions. In one case, we received information that a CBP Officer was using his position at a large urban airport to support an international drug trafficking organization. Our investigators joined a multiagency investigation, led by the ICE Office of Professional Responsibility (OPR), which resulted in the dismantling of the entire drug trafficking organization and the arrest of multiple offenders, including the CBP Officer. On at least 19 separate occasions, the CBP Officer had bypassed airport security using his own badge to smuggle money and weapons for the drug traffickers. In December 2010, he was convicted and sentenced to 8 years in prison.

A Border Patrol Agent at the Sonoita, Arizona, Border Patrol Station, was observed acting suspiciously while questioning others about the technology used to interdict smugglers. The agent had only entered on duty at Sonoita in March 2009, shortly after graduating from the Border Patrol Academy. We opened an investigation and developed evidence that the agent had sold to a purported drug trafficker sensor maps, trail maps, landmarks, and terminology used by the Border Patrol to combat smuggling. Evidence showed that on at least four occasions, the agent accepted bribes totaling

around $5,000. The agent was arrested in October 2009. On August 12, 2010, he pled guilty in Federal court to one count of bribery. On May 3, 2011, he was sentenced to 20 months incarceration, 36 months supervised release, and was ordered to pay restitution in the amount of $5,500.

Proper filing of Office of Government Ethics (OGE) forms is vital to ensuring public trust in high-level Federal officials and executive branch employees. In FY 2012, auditors observed that the ethics management function at DHS is decentralized. Ethics officials in each component's Office of Counsel are delegated the authority to implement ethics program requirements in their component. The Headquarters Ethics Office did not have internal written policies and procedures to ensure required financial disclosure reports were received, reviewed, and certified within the timelines established by OGE. The auditors discovered that some employees were submitting forms late, ethics officials were not certifying them timely, and in some cases, employees did not submit the required forms.

Additionally, TSA reported that an attorney-advisor had backdated employee public financial disclosure forms provided to the auditors in the prior year so the forms appeared to comply with the OGE requirements. According to a DHS ethics official, TSA's management acted promptly to report this information and to rescind the attorney's ethics authority and to reassign the attorney, as well as his first and second line supervisors to other work. The attorney subsequently resigned from TSA on the day he was scheduled to be interviewed by TSA's Office of Inspection.

Accomplishments

Within DHS, the primary authority for investigating allegations of criminal misconduct by DHS employees lies with OIG; ICE OPR has authority to investigate those allegations involving employees of ICE and CBP. The components play a crucial, complementary role to our, as well as, ICE OPR investigative function. The components focus on preventive measures to ensure the integrity of the DHS workforce through robust pre-employment screening of applicants, including polygraph examinations at CBP; thorough background investigations of employees; and integrity and security briefings that help employees recognize corruption signs and dangers. These preventive measures are critically important in fighting corruption and work hand-in-hand with OIG's criminal investigative activities.

Congress recognized the importance of these complementary activities by enacting the *Anti-Border Corruption Act of 2010.* This Act requires CBP, by January 4, 2013, to administer applicant screening polygraph examinations to all applicants for employment in law enforcement positions prior to hiring. CBP met this goal in October 2012. The Act also requires CBP to initiate timely periodic background reinvestigations of CBP

personnel. Agency statistics reveal that CBP declares 60 percent of applicants who are administered a polygraph examination unsuitable for employment because of prior drug use or criminal histories.

It is important to emphasize that the vast majority of employees within DHS are dedicated civil servants focused on protecting the Nation. Less than one percent of employees have committed criminal acts or other egregious misconduct.

Cyber Security

Overview

Cyber security is our Nation's firewall because it is always on alert for constant threats to networks, computers, programs, and data. It contains technologies, processes, and practices that protect our systems from attack, damage, or unauthorized access.

Challenges

In FY 2012, we reviewed the Department's efforts to guide components on securing portable devices that connect to networks, as well as how several components were applying this guidance; examined threats to IT security, including those from international and insider sources; and performed the annual *Federal Information Security Management Act of 2002* (FISMA), as amended, audit for the Department to determine its compliance with the development, documentation, and implementation of a DHS-wide information security program.

Portable Device Security

In a June 2012 audit, we determined that DHS still faced challenges using portable devices to carry out its mission and increase the productivity of its employees.[36] For example, some components had not developed policies and procedures to govern the use and accountability of portable devices. Unauthorized devices were also connected to workstations at selected components. Finally, DHS had not implemented controls to mitigate the risks associated with the use of portable devices or to protect the sensitive information that these devices store and process.

Another June report showed weaknesses in the component-wide adoption of FEMA's automated property management system, reporting of lost and stolen laptops,

[36] DHS-OIG, *DHS Needs To Address Portable Device Security Risks* (OIG-12-88, June 2012).

implementation of hard drive encryption, use of a standardized laptop image, timely installation of security patches, documentation of laptop sanitization, and accounting for wireless networks.[37] These weaknesses put laptops and the sensitive information stored and processed on them at risk of exploitation.

In a May 2012 audit, we reported that USCIS' laptop controls did not sufficiently safeguard its laptops from loss or theft and did not protect the data on the laptops from disclosure.[38] Specifically, USCIS did not have an accurate and complete inventory of its laptops, and its inventory data was not reported accurately and consistently in electronic databases. Additionally, many laptops were not assigned to specific users; USCIS did not provide adequate physical security for its laptops; and not all of USCIS' laptops used the latest encryption software or operating systems and associated service packs.

International Threats

In August 2012, we reported that the NPPD Office of Cybersecurity and Communications needed to establish and implement a plan to further its international affairs program with other countries and industry to protect cyberspace and critical infrastructure.[39] For more efficient and effective operations, NPPD should streamline its international affairs functions to coordinate foreign relations better and consolidate resources. In addition, the United States Computer Emergency Readiness Team needs to strengthen its communications and information-sharing activities with and among its counterparts to promote international incident response and the sharing of best practices.

Although TSA has shown progress, it can further develop its cyber security program by implementing insider threat policies and procedures, a risk management plan, and insider threat specific training and awareness programs for all employees. TSA can also strengthen its situational awareness security posture by centrally monitoring all information systems and augmenting current controls to better detect or prevent instances of unauthorized removal or transmission of sensitive information outside of its network.[40]

Federal Information Security Management Act

[37] DHS-OIG, *Progress Has Been Made in Securing Laptops and Wireless Networks at FEMA* (OIG-12-93, June 2012).
[38] DHS-OIG, *U.S. Citizenship and Immigration Services' Laptop Safeguards Need Improvements* (OIG-12-83, May 2012).
[39] DHS-OIG, *DHS Can Strengthen Its International Cybersecurity Programs* (OIG-12-112, August 2012).
[40] DHS-OIG, *Transportation Security Administration Has Taken Steps To Address the Insider Threat But Challenges Remain* (OIG-12-120, September 2012).

Although the Department's efforts have resulted in some improvements in its security program, components are still not executing all Department's policies, procedures, and practices. DHS needs to improve its oversight of the components' implementation of its policies and procedures to ensure that all information security weaknesses are tracked and remediated, and to enhance the quality of system authorizations. Other information security program areas also need improvement including configuration management, incident detection and analysis, specialized training, account and identity management, continuous monitoring, and contingency planning.

Accomplishments

DHS and its components have taken actions to govern, track, categorize, and secure portable devices in support of their missions. Specifically, DHS and some components have developed policies, procedures, and training on the use of portable devices. Additionally, some components include portable devices as part of overall accountable personal property inventory. FEMA has improved its inventory and configuration management controls to protect its laptop computers and the sensitive information it stores and processes. It has also implemented technical controls to protect the information stored on and processed by its wireless networks and devices.
Threats to, and emanating from, cyberspace are borderless and require robust engagement and strong partnerships with countries around the world. Thus, the NPPD has established multiple functions to support its international affairs program, to promote cyber security awareness and foster collaboration with other countries and organizations. To foster collaboration and develop international cyber security partnerships, NPPD and its subcomponents participate in international cyber exercises, capacity building workshops, and multilateral and bilateral engagements. The directorate also uses innovative technologies to share cyber data with its partner nations.

TSA's progress in addressing the IT insider threat is evidenced by its agency-wide Insider Threat Working Group and Insider Threat Section responsible for developing an integrated strategy and program to address insider threat risk. Further, TSA conducted insider threat vulnerability assessments that included personnel, physical, and information systems at selected airports and offsite offices, as well as reviews of privileged user accounts on TSA unclassified systems. Additionally, TSA has strengthened its Security Operations Center responsible for day-to-day protection of information systems and data that can detect and respond to insider threat incidents.

The *Federal Information Security Management Act* evaluation showed that the Department continued to improve and strengthen its security program.[41] Specifically,

[41] Title III of the *E-Government Act of 2002*, Public Law 107-347.

DHS implemented a performance plan to improve in four key areas: remediation of weaknesses in plans of action and milestones, quality of certification and accreditation, annual testing and validation, and security program oversight.

OIG Focus in 2013

In planning projects for FY 2013, we have placed particular emphasis on major management challenges, while aligning our work with DHS' missions and priorities in its *Strategic Plan for Fiscal Years 2012 Through 2016.* In addition, we will respond to legislative mandates, as well as undertake congressionally requested projects that may arise. DHS' mission is to prevent terrorism and enhance security, secure and manage our borders, enforce and administer our immigration laws, safeguard and secure cyberspace, and ensure resilience to disaster. The Department places priority on providing essential support to national and economic security and on maturing and becoming stronger.

In the mission areas of intelligence, transportation security, border security, infrastructure protection, and disaster preparedness and response, we are planning reviews of TSA, CBP, and FEMA, among other components and directorates. In addition to projects already in progress, our upcoming work will cover various aspects of airport security and passenger screening, securing our land borders, and disaster assistance. We also have work underway and are planning to review programs at USCIS, the USCG, and ICE. In the area of accountability, we are examining or plan to examine DHS' and its component's and directorate's controls over acquisitions and critical financial systems and data, information security, privacy stewardship, management of disaster preparedness grants, and cyber security, among other mandated and discretionary reviews.

Although not all planned projects may be completed in the upcoming fiscal year, we will continue to work with DHS to enhance effectiveness and efficiency and prevent waste, fraud, and abuse.

Appendix A
Management Comments to the Draft Report

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

Homeland Security

November 1, 2012

Charles K. Edwards
Acting Inspector General
Office of Inspector General
U.S. Department of Homeland Security
245 Murray Lane SW, Building 410
Washington, DC 20528

Re: OIG Draft Report: "Major Management Challenges Facing the Department of Homeland Security, Fiscal Year (FY) 2012" (Project No. 12-169-AUD-NONE)

Dear Mr. Edwards:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG's) perspective on the most serious management and performance challenges facing the Department. A more detailed response is provided in the Department's FY 2012 *Annual Financial Report (AFR)*.

This month marks the tenth anniversary of the creation of DHS, the largest federal reorganization since the formation of the Department of Defense. Since its inception, DHS has made significant progress becoming a more effective and integrated Department, strengthening the homeland security enterprise, and building a more secure America that is better equipped to confront the range of threats our Nation faces. As Secretary Napolitano has stated, "America is a stronger, safer, and more resilient country because of the work DHS and its many partners do every day."

The Department continues to grow and mature by strengthening and building upon existing capabilities, enhancing partnerships across all levels of government and with the private sector, and streamlining operations and increasing efficiencies within its five key mission areas: (1) preventing terrorism and enhancing security, (2) securing and managing our borders, (3) enforcing and administering our immigration laws, (4) safeguarding and securing cyberspace, and (5) ensuring resilience to disasters.

Through frameworks such as the *Quadrennial Homeland Security Review*, *Bottom-Up Review*, and *DHS Strategic Plan for FYs 2012–2016*, DHS has developed and implemented a comprehensive, strategic management approach to enhance Department-wide maturation and integration. DHS has also made significant progress to integrate and transform its management functions through the *Integrated Strategy*, first published in January 2011, which presents a clear roadmap to transform management by enhancing both vertical and horizontal integration. The strategy focuses on *all* management disciplines, especially human capital, acquisition, and financial management.

The Under Secretary for Management has led the Department-wide effort to coalesce, or integrate, the Department's management infrastructure. The Department's strategy for the past 2 years has been to make substantial progress to implement 18 specific initiatives, each with clear action plans and performance metrics. By doing so, the degree of risk has been reduced proportionately and the Department is moving closer to a transformative state. To date, nearly 65 percent of the stated outcomes have been "mostly" or "fully" addressed and the Department is on track to meet the outcome goals for the remaining outcome metrics.

Again, thank you for the opportunity to review and comment on this draft report. This report and the Department's detailed management response to the issues identified will be included in the Department's FY 2012 AFR, as required by law. Technical comments on the draft were previously provided under separate cover for OIG consideration.

Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

2

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Acting Chief Privacy Officer

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 document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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