U.S. Department of Homeland Security Annual Performance Report

Fiscal Years 2013 – 2015

Appendix B: Program Evaluations

Homeland Security

Our Vision

We will lead efforts to achieve a safe, secure, and resilient homeland.

Our Missions

We will prevent terrorism and enhance security; secure and manage our borders; enforce and administer our immigration laws; safeguard and secure cyberspace; and strengthen national preparedness and resilience. We will accomplish these missions while maturing and strengthening the Department of Homeland Security and the Homeland Security Enterprise.

About this Report

The U.S. *Department of Homeland Security Annual Performance Report for Fiscal Years (FY) 2013 – 2015* presents the Department's performance measures and applicable results aligned to our missions, provides the planned performance targets for FY 2014 and FY 2015, and includes information on the Department's Agency Priority Goals. The report is consolidated to incorporate our annual performance plan and annual performance report.

The *FY 2013 – 2015 Annual Performance Report* is one in a series of three reports which comprise the Department's Performance and Accountability Reports:

- ***DHS Annual Financial Report***: Delivery date – December 11, 2013, revised December 19, 2013
- ***DHS Annual Performance Report***: Delivery date – June 30, 2014
- ***DHS Summary of Performance and Financial Information:*** Delivery date – March 31, 2014

When published, all three reports will be located on our public website at: http://www.dhs.gov/performance-accountability.

For more information, contact:

Department of Homeland Security
Office of the Chief Financial Officer
Office of Program Analysis & Evaluation
245 Murray Lane, SW
Mailstop 200
Washington, DC 20528

Information may also be requested by sending an email to par@hq.dhs.gov or calling (202) 447-0333.

Homeland Security

Visit Our Website
www.dhs.gov

Table of Contents

Introduction

Independent program evaluations provide vital input to the Department of Homeland Security (DHS) as they offer insight to the performance of our programs and identify areas for improvement. These evaluations are used across the Department to look critically at how we conduct operations and to confront some of the key challenges facing the Department.

This Appendix provides, in tabular format, a list of the more significant DHS program evaluations conducted in FY 2013 by the U.S. Government Accountability Office (GAO) and the DHS Office of Inspector General (OIG). For each report, the report name, report number, date issued, summary, and a link to the publicly released report are provided.

Detailed information on the findings and recommendations of all GAO reports is available at: http://www.gao.gov/browse/a-z/Department_of_Homeland_Security,_Executive.

Detailed information on the findings and recommendations of all FY 2013 DHS OIG reports is available at: http://www.oig.dhs.gov/index.php?option=com_content&view=article&id=195&Itemid=187.

Program Evaluations

Mission 1: Prevent Terrorism and Enhance Security

Goal 1.1: Prevent Terrorist Attacks		
GAO Reports and Testimony		
Report: Air Passenger Screening: Transportation Security Administration Could Improve Complaint Processes	**Number:**	GAO-13-43
	Date:	11/15/2012
Summary: The Transportation Security Administration (TSA) receives thousands of air passenger screening complaints through five mechanisms, but does not have an agency-wide policy or consistent processes to guide receipt and use of such information. TSA has several methods to inform passengers about its complaint processes, but does not have an agency-wide policy or mechanism to ensure consistent use of these methods among commercial airports. GAO recommends that TSA, among other actions, establish (1) a consistent policy for receiving complaints, (2) a process to systematically analyze information on complaints from all mechanisms, and (3) a policy for informing passengers about the screening complaint processes and mechanisms to share best practices among airports.		
Report: Homeland Security: Civil Air Patrol Involved in Certain Missions, but DHS Should Assess the Benefits of Further Involvement	**Number:**	GAO-13-56
	Date:	11/1/2012
Summary: The Civil Air Patrol (CAP) has performed certain homeland security missions for federal, state, and local customers, but devotes the majority of its flying hours to training and youth programs. Several of CAP's mission areas fit within the Department of Homeland Security's (DHS) definition of homeland security, as found in the Quadrennial Homeland Security Review Report (QHSR)--a strategic framework for homeland security. GAO recommends that DHS, in coordination with the Air Force, cost-effectively assess the extent to which CAP can further assist DHS with future homeland security missions.		
Testimony: Homeland Security: DHS and TSA Continue to Face Challenges Developing and Acquiring Screening Technologies	**Number:**	GAO-13-469T
	Date:	5/8/2013
Summary: The Transportation Security Administration (TSA) has taken and is taking steps to address challenges related to developing, testing, and delivering screening technologies for selected aviation security programs, but challenges remain. For example, in January 2012, GAO reported that TSA faced challenges developing and meeting key performance requirements for the acquisition of advanced imaging technology (AIT)--i.e., full-body scanners. Specifically, GAO found that TSA did not fully follow Department of Homeland Security (DHS) acquisition policies when acquiring AIT, which resulted in DHS approving nationwide AIT deployment without full knowledge of TSA's revised specifications. DHS required TSA to notify DHS's Acquisition Review Board (ARB) if AIT could not meet any of TSA's five key performance parameters or if TSA changed a key performance parameter during testing. However, GAO found that the ARB approved TSA for full-scale production without reviewing the changed parameter. GAO has made recommendations to DHS and TSA in prior reports to help strengthen its acquisition processes and oversight.		
Report: Screening Partnership Program: TSA Should Issue More Guidance to Airports and Monitor Private versus Federal Screening Performance	**Number:**	GAO-13-208
	Date:	12/6/2012

Summary: Since implementation of the Screening Partnership Program (SPP) in 2004, 29 airports have applied to the program, citing various advantages and relatively few disadvantages. Of the 25 approved, 16 are participating in the program, 6 are currently in the contractor procurement process, and the remainder withdrew from participation because their commercial airline services were discontinued. In 2011, the Transportation Security Administration (TSA) denied applications for 6 airports because, according to TSA officials, the airports did not demonstrate that participation in the program would "provide a clear and substantial advantage to TSA security operations." GAO recommends that the TSA Administrator develop guidance for SPP applicants and a mechanism to monitor private versus federal screener performance.		
Report: Transportation Security: Action Needed to Strengthen TSA's Security Threat Assessment Process	**Number:**	GAO-13-629
	Date:	7/19/2013
Summary: The Transportation Security Administration's (TSA) Adjudication Center performance data show mixed results, and the center's performance measurement practices have limitations. The Adjudication Center relies on contractors to adjudicate security threat assessments and uses three primary measures to evaluate their performance--timeliness for completing adjudication, adjudication accuracy, and caseload status. GAO found that the Adjudication Center contractor met its timeliness and accuracy measures, but faced challenges in meeting its caseload measure. Two TSA offices that share responsibility for implementing security threat assessments--the Program Management Division in the Office of Intelligence and Analysis and the Adjudication Center in the Office of Law Enforcement/Federal Air Marshal Service--can improve coordination on workforce planning. TSA has been delayed in addressing risks posed by using contractors to adjudicate security threat assessments. GAO recommends that TSA, among other things: direct the Adjudication Center to calculate an accuracy rate that includes adjudicator performance for cases where applicants were both approved and disqualified; share adjudicator staffing plans among key program offices; and update its Adjudication Center workforce conversion plan and provide it to DHS for review and approval.		
Report: Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed	**Number:**	GAO-13-198
	Date:	5/8/2013
Summary: GAO's review of the pilot test aimed at assessing the technology and operational impact of using the Transportation Security Administration's (TSA) Transportation Worker Identification Credential (TWIC) with card readers showed that the test's results were incomplete, inaccurate, and unreliable for informing Congress and for developing a regulation (rule) about the readers. Challenges related to pilot planning, data collection, and reporting affected the completeness, accuracy, and reliability of the results. These issues call into question the program's premise and effectiveness in enhancing security. Congress should halt DHS's efforts to promulgate a final regulation until the successful completion of a security assessment of the effectiveness of using TWIC.		
Report: TSA Explosives Detection Canine Program: Actions Needed to Analyze Data and Ensure Canine Teams Are Effectively Utilized	**Number:**	GAO-13-239
	Date:	1/31/2013
Summary: The Transportation Security Administration (TSA), the federal agency that administers the National Canine Program (NCP), is collecting and using key data on its canine program, but could better analyze these data to identify program trends. TSA collects canine team data using the Canine Website System (CWS), a central management database. TSA uses CWS to capture the amount of time canine teams conduct training as well as searching for explosives odor, among other functions. However, TSA has not fully analyzed the data it collects in CWS to identify program		

trends and areas that are working well or in need of corrective action. Such analyses could help TSA to determine canine teams' proficiency, inform future deployment efforts, and help ensure that taxpayer funds are used effectively. GAO is recommending that TSA (1) regularly analyze data to identify program trends and areas working well or in need of corrective action, and (2) take actions to comprehensively assess the effectiveness of PSCs. If PSCs are determined to be effective, GAO is recommending that TSA coordinate with stakeholders to deploy PSC teams to the highest-risk airport locations and utilize them as intended.
DHS OIG Reports

Report: DHS' Efforts To Screen Members of Foreign Terrorist Organizations	**Number:**	OIG-13-103
	Date:	July 22, 2012
Summary: We determined DHS has policies and procedures for admitting members of Foreign Terrorist Organizations into the United States, and collaborating with other departments and agencies when screening members of Foreign Terrorist Organizations and issuing inadmissibility waivers. We are making three recommendations to enhance DHS' efforts to screen members of Foreign Terrorist Organizations.		
Report: Annual Review of the United States Coast Guard's Mission Performance (FY 2012)	**Number:**	OIG-13-122
	Date:	September 17, 2013
Summary: The objective of this review was to determine the extent to which the USCG Is maintaining its historical level of effort on non-homeland security missions. To address our objective, we reviewed the resource hours the USCG used to perform its various missions. We also reviewed the USCG's performance measures and results for each non-homeland security and homeland security mission. We did not verify the accuracy of the USCG-provided data. According to the USCG's data, the gap between resource hours for homeland security versus non-homeland security missions has narrowed from approximately 14 percent in fiscal year 2007 to approximately 4 percent in fiscal year 2012 (52 percent of resource hours for homeland security missions versus 48 percent for non-homeland security missions). The USCG reported that it met or exceeded 11 of 23 summary performance measure targets in fiscal year 2012. This includes 9 of 12 non-homeland security performance measures and 2 of 11 homeland security performance measure targets. In fiscal year 2012, the USCG funded nearly the same percentage of non-homeland security missions as homeland security missions.		
Report: DHS' Watchlisting Cell's Efforts To Coordinate Departmental Nominations	**Number:**	OIG-13-105
	Date:	5/23/2013
Summary: We reviewed the Watchlisting Cell to determine whether (1) it is timely, effective, and efficient in submitting DHS nominations; (2) the information provided to external partners is complete, accurate, and timely; (3) establishing the Watchlisting Cell has had an effect on the DHS component nomination process; and (4) the Watchlisting Cell has developed and communicated effective policies and procedures for coordinating nomination submissions within DHS. We also reviewed whether the Watchlisting Cell has developed an effective process for providing nominator certification training, quality assurance, and the oversight necessary for decentralization, and whether it has developed an effective methodology for planning and coordinating its resources. We determined that the Watchlisting Cell has had a positive effect on DHS and the interagency watchlisting community, as it increased the number and quality of DHS nominations, and provided oversight, guidance, and required watchlisting overview training to DHS components. However, it needs to develop performance metrics to improve its operational processes and to measure the effectiveness of its program initiatives. In addition, the Watchlisting Cell did not communicate effectively on its decentralization plan, and needs to determine the effect decentralized execution will have on the Watchlisting Cell's caseload and ability to provide oversight. The Watchlisting		

Cell operated without an itemized budget or a method for tracking its expenses, and is not prepared to address increases or fluctuations in its caseload.		
Report: Personnel Security and Internal Controls at TSA's Legacy Transportation Threat Assessment and Credentialing Office	**Number:**	OIG-13-05
	Date:	10/26/2012
Summary: We determined that TSA employee background investigations met Federal adjudicative standards, but were not timely. The Secure Flight Operations Center and the Security Threat Assessment Operations Adjudication Center identified potential insider threat risks; however, limited resources weaken internal control at the Security Threat Assessment Adjudication Center, and the shift and supervisory structure at the Secure Flight Operation Center uses resources inefficiently. Within the legacy Transportation Threat Assessment and Credentialing Office, there has been a pattern of poor management practices and inappropriate use of informal administrative processes to assess and address misconduct. We are making eight recommendations to improve background investigations, internal controls, staffing models, data system development coordination, and use of TSA or DHS formal complaint processes, and to establish an independent panel for legacy Transportation Threat Assessment and Credentialing employees to request review of reassignments.		
Report: Transportation Security Administration Information Technology Management Progress and Challenges	**Number:**	OIG-13-101
	Date:	6/24/2013
Summary: The TSA Chief Information Officer faces challenges in ensuring that the information technology environment fully supports TSA's mission needs. Specifically, TSA's information technology systems do not provide the full functionality needed to support its mission due to challenges with TSA's requirements gathering process. As a result, staff created manual workarounds or developed local systems to accomplish their mission. In addition, information technology support roles are not well defined or communicated, and the number of information technology support staff is not sufficient at certain field sites. Some field sites detailed employees from operational areas to fill in gaps in information technology support, which reduced the number of staff available to serve at security checkpoints and may hinder TSA's ability to carry out its mission.		
Report: Transportation Security Administration Office of Inspection's Efforts To Enhance Transportation Security	**Number:**	OIG-13-123
	Date:	9/24/2013
Summary: The Office of Inspection did not operate efficiently. Specifically, the office did not use its staff and resources efficiently to conduct cost-effective inspections, internal reviews, and covert testing. The office employed personnel classified as "criminal investigators," even though their primary duties may not have been criminal investigations as required by Federal law and regulations. These employees received premium pay and other costly benefits, although other employees were able to perform the same work at a lower cost. Additionally, the office did not properly plan its work and resource needs, track project costs, or measure performance effectively. Quality controls were not sufficient to ensure that inspections, internal reviews, and covert testing complied with accepted standards; staff members were properly trained; and work was adequately reviewed. Finally, the office could not always ensure other TSA components took action on its recommendations to improve TSA's operations. As a result of these issues with the office's cost-effectiveness and quality controls over its work products, TSA was not as effective as it could have been, and management may not be able to rely on the office's work. Additionally, the Office of Inspection may not have fully accomplished its mission to identify and address transportation security vulnerabilities. With the appropriate classification and training of staff and better use of		

resources, the office could improve the quality of its work. The appropriate number of reclassifications and more precise cost savings cannot be determined without an objective and comprehensive review of position classifications. If TSA does not make any changes to the number of criminal investigator positions, we estimate that it will cost as much as $17.5 million over 5 years for premium Law Enforcement Availability Pay. The office could realize further savings in training, travel, supplies, and other special employment benefits, including statutory early retirement, if its personnel classified as criminal investigators were reclassified to noncriminal investigator positions.		
Report: Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted)	**Number:**	OIG-13-91
	Date:	5/29/2013
Summary: We audited the Transportation Security Administration's (TSA) Screening of Passengers by Observation Techniques program. The program's intent is to screen passengers by observing their behavior in order to detect potential high-risk travelers. This program uses Behavior Detection Officers to detect passenger behaviors that may be indicative of stress, fear, or deception. Congressman Bennie Thompson requested an audit of TSA's Screening of Passengers by Observation Techniques program to determine its effectiveness, efficiency, and economy as a security screening protocol at airports. The audit objective was to determine whether TSA's Screening of Passengers by Observation Techniques program is structured to ensure that passengers at U.S. airports are screened in an objective and cost-effective manner to identify potential terrorists. Since the Screening of Passengers by Observation Techniques program began in fiscal year 2007, data provided by TSA indicate that the program has expended an estimated $878 million and has more than 2,800 full-time equivalent positions, as of September 30, 2012. However, TSA has not implemented a strategic plan to ensure the program's success. For example, TSA did not (1) assess the effectiveness of the Screening of Passengers by Observation Techniques program, (2) have a comprehensive training program, (3) ensure outreach to its partners, or (4) have a financial plan. As a result, TSA cannot ensure that passengers at United States airports are screened objectively, show that the program is cost-effective, or reasonably justify the program's expansion. In fiscal year 2012, TSA's Behavior Detection and Analysis Division developed a draft strategic plan that includes a statement of mission, goals, and objectives. However, the plan had not been approved and implemented at the time of our review. We made six recommendations to improve the effectiveness of the Screening of Passengers by Observation Techniques program. TSA concurred with all recommendations.		
Report: Transportation Security Administration's Screening Partnership Program	**Number:**	OIG-13-99
	Date:	6/30/2013
Summary: As of January 2013, 16 airports were participating in the Screening Partnership Program. Under the program, an airport operator may apply to use a private company to screen passengers and baggage rather than use Federal Government screening personnel. TSA reviews and approves applications to participate, awards contracts to private screening companies, and oversees the private screening workforce. We performed this audit to determine whether TSA administered the Screening Partnership Program in accordance with Federal regulations. Until 2011, TSA had no criteria when considering whether to approve airports' applications to participate in the Screening Partnership Program. TSA administered the program in accordance with the *FAA Modernization and Reform Act of 2012*, but could improve aspects of its administration. Specifically, TSA's files for its five most recent decisions to approve airports' applications to participate included documents that had not been finalized, as well as documents with inaccurate information. In addition, TSA did not document the rationale used to decide on four of the five contracts awarded during 2011 and 2012.		

Report: Transportation Security Administration's Deployment and Use of Advanced Imaging Technology	**Number:**	OIG-13-120
	Date:	9/16/2013

Summary: TSA began deploying advanced imaging technology in 2007 and accelerated its deployment after the attempted airplane bombing on December 25, 2009. TSA created and followed deployment schedules. However, it did not develop a comprehensive deployment strategy to ensure all advanced imaging technology units were effectively deployed and fully used for screening passengers. This condition existed because TSA did not—

- Have a policy or process requiring program offices to prepare strategic deployment plans for new technology that align with the overall goals of the Passenger Screening Program, and
- Have adequate internal controls to ensure accurate data on advanced imaging technology utilization.

Goal 1.2: Prevent and Protect Against the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities

GAO Reports

Report: Combating Nuclear Smuggling: Lessons Learned from Cancelled Radiation Portal Monitor Program Could Help Future Acquisitions	**Number:**	GAO-13-256
	Date:	6/11/2013

Summary: The advanced spectroscopic portal monitor (ASP)--a next-generation radiation portal monitor (RPM) for screening trucks and cargo containers--did not pass field validation tests conducted in 2009 and 2010. The Department of Homeland Security's (DHS) Domestic Nuclear Detection Office (DNDO) intended to replace many currently deployed RPMs and handheld radiation detectors used by U.S. Customs and Border Protection (CBP) with ASPs. However, in the tests, ASP did not meet key requirements to detect radiation and identify its source. Conducting lessons learned reviews when programs are cancelled benefits organizations by identifying things that worked well and did not work well in order to improve future acquisitions programs, according to experts GAO consulted. However, DHS does not have processes in place to ensure such reviews are conducted or that the results are disseminated. DHS should require lessons learned reviews and develop processes to ensure such reviews are done in a timely manner and the results disseminated throughout the department.

Report: Combating Nuclear Smuggling: Megaports Initiative Faces Funding and Sustainability Challenges	**Number:**	GAO-13-37
	Date:	11/28/2012

Summary: As of August 2012, the National Nuclear Security Administration (NNSA) had completed 42 of 100 planned Megaports projects in 31 countries and, as of December 2011, NNSA had spent about $850 million on the Megaports Initiative (Initiative). NNSA's Initiative has equipped these seaports with radiation detection equipment, established training programs for foreign personnel, and created a sustainability program to help countries operate and maintain the equipment. However, the administration's fiscal year 2013 budget proposal would reduce the Initiative's budget by about 85 percent, and NNSA plans to shift the Initiative's focus from establishing new Megaports to sustaining existing ones. As a result, NNSA has suspended ongoing negotiations and cancelled planned deployments of equipment in five countries. GAO recommends that NNSA take actions, including (1) finalizing its long-term plan for ensuring the sustainability of Megaports operations after NNSA's final transfer of equipment to partner countries and (2) developing and maintaining useful and reliable measures to assess the performance of the Initiative.

GAO also recommends that NNSA and DHS jointly assess the extent to which the two Initiatives

are effectively coordinating.		
Report: Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened	**Number:**	GAO-13-353
	Date:	4/5/2013
Summary: Since 2007, the Department of Homeland Security's (DHS) Infrastructure Security Compliance Division (ISCD) has assigned about 3,500 high-risk chemical facilities to risk-based tiers under its Chemical Facility Anti-Terrorism Standards (CFATS) program, but it has not fully assessed its approach for doing so. The approach ISCD used to assess risk and make decisions to place facilities in final tiers does not consider all of the elements of consequence, threat, and vulnerability associated with a terrorist attack involving certain chemicals. GAO recommends that DHS enhance its risk assessment approach to incorporate all elements of risk, conduct a peer review after doing so, and explore opportunities to gather systematic feedback on facility outreach.		
Report: Overlap and Duplication: Federal Inspections of Entities Registered with the Select Agent Program	**Number:**	GAO-13-154
	Date:	1/31/2013
Summary: About 15 percent of entities registered to work with select agents were subject to inspection overlap (multiple federal agencies inspecting within a 2-year period). Entities experiencing overlap tended to be larger ones, with more laboratories, principal investigators, and staff. Although there was overlap between Department of Transportation (DOT) inspections and those of the Centers for Disease Control and Prevention (CDC) and the Animal and Plant Health Inspection Service (APHIS), they were generally not duplicative because specific inspection activities tended to differ, according to GAO's survey of entities experiencing overlap. For example, DOT inspections tended to focus on transportation issues, such as checking hazardous materials and transportation security plans, rather than general biosafety issues. The Department of Homeland Security (DHS) and Department of Defense (DOD) inspections, however, tended to be more duplicative with those of CDC and APHIS. For example, both review the same documents, require safety and security demonstrations, conduct inventory inspections and personnel interviews, and provide corrective action plans. While inspections are important for safety and compliance, there is no value added when federal agencies are expending resources to conduct the same work and, in some cases, reinspecting before entities have had time to respond to findings from a previous inspection. GAO recommends that CDC and APHIS work with DHS and DOD to coordinate inspections and ensure consistent application of inspection standards.		
DHS OIG Reports		
Report: United States Customs and Border Protection's Radiation Portal Monitors at Seaports	**Number:**	OIG-13-26
	Date:	3/25/2013
Summary: The Domestic Nuclear Detection Office (DNDO) tests, acquires, deploys, and provides maintenance in the first year of operation; CBP provides maintenance after the first year. CBP has the lead for commissioning, operating, and maintaining the radiation portal monitors. We conducted this audit to determine whether DNDO and CBP deploy and use radiation portal monitors to ensure the most efficient cargo screening at seaports. Our audit also addressed the congressional mandate in the *Coast Guard and Maritime Transportation Act of 2004*, as amended, to conduct an annual evaluation of the cargo inspection system. DNDO reported that there are currently 444 radiation portal monitors operating at seaports throughout the U.S., which are meeting the requirement to screen all containerized cargo at the 22 seaports with the most container volume. We were unable to determine whether DNDO and CBP initially deployed radiation portal monitors to ensure operational efficiency because the components did not thoroughly document deployment decisions and plans. Although all cargo is being screened, we identified some radiation portal monitors utilized infrequently or not utilized at all. The components do not fully coordinate or		

centrally manage the radiation portal monitor program to ensure effective and efficient operations. Specifically, CBP does not consistently gather and review utilization information to ensure that it is fully utilizing all radiation portal monitors. CBP does not always monitor and promptly evaluate changes in the screening environment at seaports to relocate radiation portal monitors as necessary. Finally, DNDO and CBP do not accurately track and monitor their inventory of radiation portal monitors. Given the radiation portal monitors' limited life and the lack of funding for new monitors, CBP and DNDO should better coordinate to fully utilize, promptly relocate, and properly maintain inventory to best use resources and to continue screening of all containerized cargo entering U.S. seaports. The components concurred with our three recommendations and will identify a single program office responsible for fully coordinating and centrally managing the program; establish guidelines to track and report the utilization of monitors at every seaport; and develop and document a formal collaborative process to ensure that monitor relocation is effectively planned and implemented to meet security needs at seaports.

Report: Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	**Number:**	OIG-13-55
	Date:	2/25/2013

Summary: We assessed DHS' efforts to implement the Chemical Facility Anti-Terrorism Standards Program from inception to the end of fiscal year 2012. Specifically, we reviewed whether: (1) management controls are in place and operational to ensure that the Chemical Facility Anti-Terrorism Program is not mismanaged; (2) NPPD and Infrastructure Security Compliance Division leadership misrepresented program progress; and (3) nonconforming opinions of program personnel have been suppressed or met with retaliation. Program progress has been slowed by inadequate tools, poorly executed processes, and insufficient feedback on facility submissions. In addition, program oversight had been limited, and confusing terminology and absence of appropriate metrics led to misunderstandings of program progress. The Infrastructure Security Compliance Division still struggles with a reliance on contractors and the inability to provide employees with appropriate training. Overall efforts to implement the program have resulted in systematic noncompliance with sound Federal Government internal controls and fiscal stewardship, and employees perceive that their opinions have been suppressed or met with retaliation. Although we were unable to substantiate any claims of retaliation or suppression of nonconforming opinions, the Infrastructure Security Compliance Division work environment and culture cultivates this perception. Despite the Infrastructure Security Compliance Division's challenges, the regulated community views the Chemical Facility Anti-Terrorism Standards Program as necessary.

Goal 1.3: Reduce Risk to the Nation's Critical Infrastructure, Key Leadership, and Events

GAO Reports

Report: Critical Infrastructure Protection: An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure	**Number:**	GAO-13-11
	Date:	10/25/2012

Summary: The Department of Homeland Security (DHS) is developing a resilience policy, but an implementation strategy is a key next step that could help strengthen DHS resilience efforts. DHS defines resilience as the ability to resist, absorb, recover from, or adapt to adversity, and some high-level documents currently promote resilience as a key national goal. Specifically, two key White House documents emphasize resilience on a national level--the 2011 Presidential Policy Directive 8 and the 2012 National Strategy for Global Supply Chain Security. Since 2009, DHS has

emphasized the concept of resilience and is currently in the process of developing a resilience policy, the initial steps of which have included creating two internal entities--the Resilience Integration Team and the Office of Resilience Policy (ORP). According to ORP officials, they saw a need to establish a policy that provides component agencies with a single, consistent, department-wide understanding of resilience that clarifies and consolidates resilience concepts from high-level guiding documents, and helps components understand how their activities address DHS's proposed resilience objectives. ORP officials hope to have an approved policy in place later this year. However, DHS officials stated that currently there are no plans to develop an implementation strategy for this policy. An implementation strategy that defines goals, objectives, and activities; identifies resource needs; and lays out milestones is a key step that could help ensure that DHS components adopt the policy consistently and in a timely manner. For example, an implementation strategy with goals and objectives could provide ORP with a more complete picture of how DHS components are implementing this policy.		
Report: Critical Infrastructure Protection: DHS Could Strengthen the Management of the Regional Resiliency Assessment Program	**Number:**	GAO-13-616
	Date:	7/30/2013
Summary: The Department of Homeland Security (DHS) has developed nine criteria that consider various factors--including the willingness of various stakeholders, such as asset owners and operators, to participate and concentrations of high-risk critical infrastructure--when identifying possible locations for Regional Resiliency Assessment Program (RRAP) projects. According to DHS officials, final project selections are then made from a list of possible locations based on factors including geographic distribution and DHS priorities, among other considerations. However, it is unclear why some RRAP projects are recommended over others because DHS does not fully document why these decision are made. Federal internal control standards call for agencies to promptly record and clearly document transactions and significant events. Because DHS's selection process identifies a greater number of potential projects than DHS has the resources to perform, documenting why final selections are made would help ensure accountability, enabling DHS to provide evidence of its decision making. GAO recommends that DHS document final RRAP selections and develop a mechanism to measure whether RRAP participation influences facilities to make RRAP-related enhancements.		
Report: Passenger Rail Security: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives	**Number:**	GAO-13-20
	Date:	12/19/2012
Summary: The Transportation Security Administration (TSA) has inconsistently overseen and enforced its rail security incident reporting requirement because it does not have guidance and its oversight mechanisms are limited, leading to considerable variation in the types and number of incidents reported. Though some variation is expected in the number and type of incidents reported because of differences in rail agency size, location, and ridership, local TSA inspection officials have provided rail agencies with inconsistent interpretations of the reporting requirement. GAO recommends, among other things, that TSA (1) develop guidance on the types of incidents that should be reported, (2) enhance existing oversight mechanisms for compliance inspections and enforcement actions, (3) develop guidance to reduce errors from data entry problems, and (4) establish a process for regularly conducting trend analysis of incident data.		
Report: Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress	**Number:**	GAO-13-296
	Date:	3/25/2013

Summary: The Department of Homeland Security (DHS) has made several changes to its criteria for including assets on the National Critical Infrastructure Prioritization Program (NCIPP) list of the nation's highest-priority infrastructure, but has not identified the impact of these changes or validated its approach. In 2009, DHS changed the criteria to make the list entirely consequence based--that is, based on the effect of an event on public health and safety, and economic, psychological, and government mission impacts. Subsequent changes introduced specialized criteria for some sectors and assets. For example, infrastructure that has received a specific, credible threat, but otherwise does not meet NCIPP criteria, may be included on the list. DHS's changes to the NCIPP criteria have changed the composition of the NCIPP list, which has had an impact on users of the list, such as the Federal Emergency Management Agency. However, DHS has not reviewed the impact of changes on users nor validated its approach to developing the list. While the change to an entirely consequence-based list created a common approach to identify infrastructure and align the program with applicable laws and the National Infrastructure Protection Plan, recent criteria changes to accommodate certain sectors and assets represent a departure from this common approach, which could hinder DHS's ability to compare infrastructure across sectors. GAO recommends that DHS commission an external peer review and develop an approach to verify that the annual reports are provided to the requisite committees of Congress.		
Report: Facility Security: Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies	**Number:**	GAO-13-222
	Date:	2/20/2013
Summary: Agencies draw upon a variety of information sources in developing and updating their physical security programs. The most widely used source, according to survey responses from 32 agencies, is the institutional knowledge or subject matter expertise in physical security that agencies' security staff have developed through their professional experience. The second most used source are standards issued by the Interagency Security Committee (ISC). The standards, which are developed based on leading security practices across the government, set forth a decision-making process to help ensure that agencies have effective physical security programs in place. However, according to survey responses, the extent of agencies' use of ISC standards varied--with some agencies using them in a limited way. DHS should direct ISC to conduct outreach to executive branch agencies to clarify how its standards are to be used, and develop and disseminate guidance on management practices for resource allocation as a supplement to ISC's existing physical security standards.		

Mission 2: Secure and Manage Our Borders

Goal 2.1: Secure U.S. Air, Land, and Sea Borders and Approaches		
GAO Reports		
Report: Border Patrol: Key Elements of New Strategic Plan Not Yet in Place to Inform Border Security Status and Resource Needs	**Number:**	GAO-13-25
	Date:	1/9/2013
Summary: In fiscal year 2011, the Department of Homeland Security (DHS) reported data meeting its goal to secure the land border with a decrease in apprehensions; our data analysis showed that apprehensions decreased within each southwest border sector and by 68 percent in the Tucson sector from fiscal years 2006 to 2011, due in part to changes in the U.S. economy and achievement of Border Patrol strategic objectives. These data generally mirrored the decrease in estimated known illegal entries across locations. Border Patrol sectors assess how effectively they use resources to secure the border, but differences in how sectors collect and report the data preclude comparing results. Border Patrol issued guidance in September 2012 to improve the consistency of sector data collection and reporting, which may allow future comparison of performance. GAO recommends that CBP ensure Border Patrol develops milestones and time frames for developing border security goals and measures to assess progress made and resource needs.		
Report: Border Security: Partnership Agreements and Enhanced Oversight Could Strengthen Coordination of Efforts on Indian Reservations	**Number:**	GAO-13-352
	Date:	4/5/2013
Summary: The Department of Homeland Security (DHS) is coordinating in a variety of ways with tribes, such as through joint operations and shared facilities and Operation Stonegarden--a DHS grant program intended to enhance coordination among local, tribal, territorial, state, and federal law enforcement agencies in securing United States borders. However, the Border Patrol and tribes face coordination challenges. Officials from five tribes reported information-sharing challenges with the Border Patrol, such as not receiving notification of federal activity on their lands. Border Patrol officials reported challenges navigating tribal rules and decisions. GAO recommends that DHS examine the benefits of government-to-government agreements with tribes and develop and implement a mechanism to monitor border security coordination efforts with tribes.		
Report: Southwest Border Security: Data Are Limited and Concerns Vary about Spillover Crime along the Southwest Border	**Number:**	GAO-13-175
	Date:	2/26/2013
Summary: The Federal Bureau of Investigation's (FBI) Uniform Crime Reporting (UCR) Program, the government's centralized repository for crime data, provides the only available standardized way to track crime levels in border counties over time. However, UCR data lack information on whether reported offenses are attributable to spillover crime, and have other limitations, such as underreporting to police. Also, UCR data cannot be used to identify links with crimes often associated with spillover from Mexico, such as cartel-related drug trafficking. Cognizant of these limitations, GAO's analysis of data for southwest border counties with sufficiently complete data show that, generally, both violent and property crimes were lower in 2011 than in 2004. For example, the violent crime rate in three states' border counties was lower by at least 26 percent in 2011 than in 2004 and in one other state lower by 8 percent in 2011 than in 2005.		

DHS OIG Reports		
Testimony: Border Security: Examining Provisions In The Border Security, Economic Opportunity, and Immigration Modernization Act	**Number:**	Testimony
	Date:	1/29/2013
Summary: Through our audits and reviews, we have identified a number of challenges that DHS must overcome to secure our borders and establish effective immigration policies and processes. Some of these challenges are a result of differing legacy systems and programs that need to be integrated and coordinated among the components and with stakeholders outside of the Department. Other challenges are related to inadequate strategic planning, a dearth of performance measures, and data and information that cannot be relied on to make sound decisions. It is important to note that, based on the Department's response to our numerous reports, it is clear that it is diligently working to address these issues. However, it takes time to develop strategic plans, improve information systems, revise and update guidance, implement and disseminate new policies and procedures, and correct the underlying data. This can be particularly time-consuming when, as is usually the case, such plans, policies, and procedures require coordination and concurrence among multiple entities, including some outside of DHS and its components. Competing and changing priorities and funding uncertainties also affect the Department's ability to address these issues.		
Report: DHS Involvement in OCDETF Operation Fast and Furious	**Number:**	OIG-13-49
	Date:	3/22/2013
Summary: Within the Department of Homeland Security, under the Foreign Military Sales program, the United States Coast Guard (USCG) procures and provides defense-related articles and services to foreign governments, and U.S. Customs and Border Protection (CBP) controls exports of articles related to Foreign Military Sales. In February 2013, the U.S. Government Accountability Office deemed Foreign Military Sales a high risk area for the Federal Government. We performed this audit to determine whether CBP and the USCG have adequate controls over the Foreign Military Sales export process. CBP and the USCG need to improve their controls over exports related to Foreign Military Sales. CBP has a process to assess the risk associated with exports and target shipments for physical inspection. However, during this process officers rely on potentially unverified and inaccurate information that shippers submit to an export database. Additionally, according to officers at the two ports we reviewed, they did not physically inspect any Foreign Military Sales-related exports in fiscal year 2012. CBP also does not have a centralized system to track Foreign Military Sales-related exports, which increases the risk of unauthorized exports and diminishes the efficiency of the process. CBP's guidance to the ports for handling Foreign Military Sales-related shipments is outdated, and the component does not provide formal training to its officers on handling these exports. Of the USCG contracts for Foreign Military Sales articles that we reviewed, not all specified that they were related to the program, nor did they all include Foreign Military Sales requirements. Foreign Military Sales regulations do not require operating agencies, such as the USCG, to verify accuracy of shipment documentation in the Automated Export System that CBP uses to assess risk and target shipments for physical inspections. Therefore, the USCG may be unaware of inaccurate Foreign Military Sales-related shipment documentation in the system.		
Report: DHS' H-60 Helicopter Programs (Revised)	**Number:**	OIG-13-89
	Date:	May 23, 2013
Summary: The Department of Homeland Security (DHS) has 62 H-60 helicopters operated by U.S. Customs and Border Protection (CBP) and the United States Coast Guard (USCG), both of		

which are converting the helicopters to add about 15 years of operational life. The USCG properly managed its H-60 helicopter program, but CBP did not. Most of the CBP H-60s were on loan from the United States Army (Army), and CBP had an Inter-Agency Agreement with the Army to complete all the conversions and modifications. CBP did not properly manage or oversee its H-60 program, which affected the cost effectiveness and timely delivery of converted and modified H-60 helicopters. Between September 2008 and July 2012, the Army converted and modified two CBP H-60s at an average cost of $22.3 million each, and each conversion was completed in about 1,300 days. OIG estimates that each future CBP conversion will cost approximately $18.3 million and will take about 620 days to complete. Between January 2007 and July 2012, the USCG converted 27 of its H-60s, and the last 7 USCG conversions cost approximately $5.3 million each and took an average of 301 days to complete. As a result, the Department and CBP increased costs and experienced delays in converting and modifying CBP's H-60 fleet. These delays have already limited CBP's operation of its H-60s, and CBP anticipates that it may not be able to fly up to nine of its H-60s beginning in 2014. However, if DHS directs CBP and the USCG to complete the remaining 11 CBP H-60 conversions and modifications at the USCG Aviation Logistics Center, DHS could save about $126 million and have CBP H-60s able to fly 7 years sooner than anticipated. We made four recommendations that, when implemented, should improve the Department's management and oversight of its aviation assets, as well as CBP's aviation acquisitions and its H-60 program. DHS concurred with three of the four recommendations.

Goal 2.2: Safeguard and Expedite Lawful Trade and Travel		
GAO Reports and Testimony		
Report: Agricultural Quarantine Inspection Feeds: Major Changes Needed to Align Fee Revenues with Program Costs	**Number:**	GAO-13-268
	Date:	3/1/2013
Summary: GAO's analysis of the Agricultural Quarantine Inspection (AQI) fee and cost data revealed a more than $325 million gap between fee revenues and total program costs in fiscal year 2011, or 38 percent of AQI program costs. The program, which is co-administered by the Department of Agriculture (USDA) Animal and Plant Health Inspection Service (APHIS) and Department of Homeland Security (DHS) Customs and Border Patrol (CBP), has a gap for several reasons: 1) APHIS's authority does not permit it to charge all persons seeking entry to the United States (e.g., pedestrians) and does not permit it to charge the costs of those inspections to others; 2) APHIS has chosen not to charge some classes of passengers, citing administrative fee collection difficulties; 3) CBP does not charge a portion of all primary inspections to agriculture functions, as required by CBP guidance; 4) APHIS does not consider all imputed costs (that is, costs incurred by other agencies on behalf of the AQI program) when setting fees; and 5) the allowable rates for overtime services are misaligned with the personnel costs of performing those services. APHIS is considering fees that would better align many, but not all, AQI fees with related inspection activity costs. GAO is making a number of recommendations aimed at more fully aligning fees with program costs, aligning the division of fees between APHIS and CBP with their respective costs, and ensuring that fees are collected when due. Further, GAO suggests Congress amend the AQI fee authority to allow the Secretary of Agriculture to set fee rates to recover the full costs of the AQI program.		
Report: Homeland Security: Agriculture Inspection Program Has Made Some Improvements, but Management Challenges Persist	**Number:**	GAO-12-885
	Date:	10/15/2012
Summary: The Department of Homeland Security (DHS) and the U.S. Department of Agriculture		

(USDA) have taken steps to implement all seven of the recommendations GAO made in 2006 to improve the Agriculture Quarantine Inspection (AQI) program, but they face challenges in fully implementing four of them. Specifically, DHS and USDA have implemented GAO's recommendations to improve information sharing, review DHS's financial management system for the AQI program, and remove barriers to timely and accurate transfers of AQI user fees--collected for AQI services provided in connection with the arrival of international air passengers and conveyances at U.S. ports. However, DHS and USDA face challenges in fully implementing GAO's recommendations to adopt meaningful performance measures, establish a national risk-based staffing model, improve the agriculture canine program, and revise user fees to cover program costs. GAO recommends, among other things, that (1) DHS and USDA develop a joint strategic plan for the AQI program, (2) DHS develop a plan for implementing a staffing model, and (3) DHS and USDA take steps to improve the reliability of certain data.		
Testimony: Border Security: Additional Actions Needed to Improve Planning for a Biometric Air Exit System	**Number:**	GAO-13-853T
	Date:	9/26/2013
Summary: GAO concluded in its July 2013 report that without robust planning that includes time frames and milestones to develop and implement an evaluation framework for this assessment, DHS lacks reasonable assurance that it will be able to provide this assessment to Congress for the fiscal year 2016 budget cycle as planned. Furthermore, any delays in providing this information to Congress could further affect possible implementation of a biometric exit system to address statutory requirements. Therefore, GAO recommended that the Secretary of Homeland Security establish time frames and milestones for developing and implementing an evaluation framework to be used in conducting the department's assessment of biometric exit options.		
Report: Supply Chain Security: CBP Needs to Conduct Regular Assessments of Its Cargo Targeting System	**Number:**	GAO-13-9
	Date:	11/26/2012
Summary: U.S. Customs and Border Protection (CBP), within the Department of Homeland Security (DHS), employs a risk-based approach that uses the Automated Targeting System (ATS) and other tools to identify (target) maritime cargo shipments for further examination. ATS is a web-based enforcement and decision support system that includes a set of rules to assess the risk level for each arriving cargo shipment. This set of rules is referred to as the maritime national security weight set (weight set) because each rule in the set has a specific weighted value assigned to it. CBP classifies the risk scores from the weight set as low, medium, or high risk. CBP policy states that a shipment's risk score is to determine, in part, actions taken by CBP officers (targeters) at the ports. Specifically, targeters are generally required to review shipment data for all medium-risk and high-risk shipments and hold high-risk shipments for examination. The risk score, however, is not the sole factor that determines whether a targeter reviews the data for a shipment or whether CBP examines a shipment. In particular, targeters at each of the six ports GAO visited explained that they use the ATS risk score as a starting point for the targeting process but that their decisions regarding which shipments to examine are ultimately based on additional research. Targeters at the six ports GAO visited said they also use tools outside of ATS, such as web searches, to research shipments. GAO recommends that CBP (1) ensure that future updates to the weight set are based on assessments of its performance and (2) establish targets for performance measures and use those measures to regularly assess effectiveness of the weight set.		
Report: Supply Chain Security: DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports	**Number:**	GAO-13-764
	Date:	9/16/2013
Summary: Department of Homeland Security (DHS) components have developed models to assess the risks of foreign ports and cargo, but not all components have applied risk management		

principles to assess whether maritime security programs cover the riskiest ports. The U.S. Coast Guard uses its risk model to inform operational decisions for its International Port Security (IPS) program and annually updates its assessment. In contrast, U.S. Customs and Border Protection (CBP) has not regularly assessed ports for risks to cargo under its Container Security Initiative (CSI) program. CBP's selection of the initial 23 CSI ports was primarily based on the volume of U.S.-bound containers, but beginning in 2003, CBP considered more threat information when it expanded the number of CSI ports. CBP has not assessed the risk posed by foreign ports that ship cargo to the United States for its CSI program since 2005. GAO recommends that CBP periodically assess the supply chain security risks from foreign ports that ship cargo to the United States and use the results to inform any future expansion of CSI and determine whether changes need to be made to existing CSI ports.		
Report: U.S.-Mexico Border: CBP Action Needed to Improve Wait Time Data and Measure Outcomes of Trade Facilitation Efforts	**Number:**	GAO-13-603
	Date:	7/24/2013
Summary: Within the Department of Homeland Security (DHS), U.S. Customs and Border Protection's (CBP) data on commercial vehicle wait times--the time it takes to travel from the end of the queue to the CBP primary inspection point at land border crossings--are unreliable for public reporting and CBP management decisions across border crossings. These data--which are collected manually by CBP officers--are unreliable because CBP officers inconsistently implement an approved data collection methodology, and the methodologies used vary by crossing. GAO recommends that CBP (1) determine and take steps to help ensure consistent implementation of existing wait time data collection methodologies, (2) assess the feasibility of replacing current methodologies with automated methods, (3) document its staff allocation process and rationale, and (4) develop outcome-oriented performance measures.		
DHS OIG Reports		
Report: CBP's and USCG's Controls Over Exports Related to Foreign Military Sales	**Number:**	OIG-13-119
	Date:	9/9/2013
Summary: The Department of Homeland Security (DHS) had minimal involvement in the Organized Crime and Drug Enforcement Task Force Operation Fast and Furious. Our review of DHS involvement in the operation determined that senior DHS officials in Washington, DC had no awareness of the methodology used by the task force to investigate Operation Fast and Furious until media reports were published in March 2011. These reports asserted that while investigating an international weapons smuggling ring, task force members used a dangerous methodology in which they observed suspicious weapons purchases, but took no effective action to seize the weapons. As a result, weapons were smuggled to Mexican drug trafficking organizations. Similarly, U.S. Immigration and Customs Enforcement (ICE) headquarters officials did not learn about the methodology until December 2010, when the operation was almost over. A Homeland Security Investigations Arizona official informed Homeland Security Investigations headquarters officials that two of these weapons were found at the scene of the murder of a U.S. Border Patrol Agent. However, the officials did not inform ICE headquarters staff that a Homeland Security Investigations special agent participated in the operation.		

Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors		
GAO Reports		
Report: Registered Sex Offenders: Sharing More Information Will Enable Federal Agencies to Improve Notifications of Sex Offenders' International Travel	**Number:**	GAO-13-200
	Date:	2/14/2013
Summary: Three federal agencies--U.S. Marshals, International Criminal Police Organization (INTERPOL) Washington - U.S. National Central Bureau (USNCB), and U.S. Immigration and Customs Enforcement (ICE)--use information from state, local, territorial, and tribal jurisdictions, as well as passenger data from the U.S. Customs and Border Protection (CBP), to identify registered sex offenders traveling outside of the United States. Similarly, these agencies may be notified of registered sex offenders traveling to the United States through several means, including tips from foreign officials or when CBP queries the registered sex offender's biographic information at a port of entry and finds that the offender has a criminal history. However, none of these sources provides complete or comprehensive information on registered sex offenders leaving or returning to the United States. GAO recommends that ICE consider receiving the automated notifications and DOJ and DHS take steps to ensure that USNCB and ICE (1) have information on the same number of traveling registered sex offenders and (2) have access to the same level of detail about each traveling registered sex offender.		

Mission 3: Enforce and Administer Our Immigration Laws

Goal 3.1: Strengthen and Effectively Administer the Immigration System

GAO Reports

Report: Department of Homeland Security: Provisional Unlawful Presence Waivers of Inadmissibility for Certain Immediate Relatives	**Number:**	GAO-13-288R
	Date:	1/16/2013

Summary: GAO reviewed the Department of Homeland Security's (DHS) new rule on provisional unlawful presence waivers of inadmissibility for certain immediate relatives. GAO found that (1) the final rule implements the provisional unlawful presence waiver process, by allowing certain immediate relatives of U.S. citizens who are physically present in the United States to request provisional unlawful presence waivers prior to departing from the United States for consular processing of their immigrant visa applications; and (2) DHS complied with applicable requirements in promulgating the rule.

Report: H-2A Visa Program: Modernization and Improved Guidance Could Reduce Employer Application Burden	**Number:**	GAO-12-706
	Date:	10/15/2012

Summary: Over 90 percent of employer applications for H-2A workers were approved in fiscal year (FY) 2011, but some employers experienced processing delays. For example, the Department of Labor (Labor) processed 63 percent of applications in a timely manner in FY 2011, but 37 percent were processed after the deadline, including 7 percent that were approved less than 15 days before workers were needed. This left some employers little time for the second phase of the application process, which is managed by the Department of Homeland Security (DHS), and for workers to obtain visas from the Department of State (State). Although workers can apply for visas online, most of the H-2A process involves paper handling, which contributes to processing delays. In addition, employers who need workers at different times of the season must repeat the entire process for each group of workers. Although the agencies lack data on the reasons for processing delays, employers reported delays due to increased scrutiny by Labor and DHS when these agencies implemented new rules and procedures intended to improve program integrity and protect workers. For example, in FY 2011, Labor notified 63 percent of employers that their applications required changes or additional documentation to comply with its new rules, up sharply from previous years. GAO recommends that (1) Labor and DHS use their new electronic application systems to collect data on reasons applications are delayed and use this information to improve the timeliness of application processing; (2) Labor allow employers to submit one application for groups of similar workers needed in a single season; and (3) Labor review and revise, as appropriate, its guidance to states regarding methods for determining the acceptability of employment practices in employers' applications.

DHS OIG Reports

Report: Improvements Needed for SAVE to Accurately Determine Immigration Status of Individuals Ordered Deported	**Number:**	OIG-13-11
	Date:	12/7/2012

Summary: The Systematic Alien Verification for Entitlements program provided information that was sometimes outdated and erroneous about an individual's immigration status to benefit-granting agencies. This occurred because status codes in the Central Index System were generally not updated when the Immigration Court issued a decision to remove, deport, or exclude an individual from the United States. Instead, the codes were updated when the individual physically left the

United States, which can take years. This problem could potentially affect the more than 800,000 individuals who have been ordered deported, removed, and excluded but who are still in the United States. Although the Systematic Alien Verification for Entitlements response in and of itself did not automatically result in approval of financial or other benefits by Federal, State, and local agencies, an erroneous response could result in agencies granting benefits to unentitled individuals. Our random statistical sample tests of individuals who had been ordered deported but still remained in the United States identified a 12 percent error rate in immigration status verification. In other words, these individuals had no status, but were erroneously identified as having lawful immigration status. The remaining 88 percent passed our tests because the individuals had lawful immigration status at the time of status verification. This includes situations where the individual (1) was ordered deported after the verification or (2) obtained permanent or temporary status after being ordered deported but before the status verification. Benefits for which individuals were verified ranged from airport badges and Transportation Worker Identification Cards, which provide individuals with access to secure areas, to food stamps, driver's licenses, and education assistance. Some individuals included in our sample had committed felonies ranging from citizenship fraud to aggravated assault.

Report: U.S. Citizenship and Immigration Services' Tracking and Monitoring of Potentially Fraudulent Petitions and Applications for Family-Based Immigration Benefits	**Number:**	OIG-13-97
	Date:	6/12/2013
Summary: USCIS has procedures to track and monitor documentation related to petitions and applications for family-based immigration benefits suspected of being fraudulent. However, once family-based immigration petitions and applications were investigated and adjudicated, fraud-related data were not always recorded and updated in appropriate electronic databases to ensure their accuracy, completeness, and reliability. Specifically, FDNS personnel did not record in appropriate electronic databases all petitions and applications denied, revoked, or rescinded because of fraud. Supervisors also did not review the data entered into the databases to monitor case resolution. Without accurate data and adequate supervisory review, USCIS may have limited its ability to track, monitor, and identify inadmissible aliens, and to detect and deter immigration benefit fraud.		
Report: Implementation of L-1 Visa Regulations	**Number:**	OIG-13-107
	Date:	11/2/2012
Summary: The VWPO has developed and implemented standard operating procedures and evaluation criteria that ensure that the objectives for conducting initial and continuing designation reviews, as mandated by Congress, are met. In addition, the VWPO has engaged in on-going communication and effective collaborations with DOS and DOJ officials during each phase of the VWP review process.		

Goal 3.2: Prevent Unlawful Immigration

GAO Reports and Testimony

Report: Overstay Enforcement: Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Air Exit Program	**Number:**	GAO-13-683
	Date:	7/30/2013
Summary: Since April 2011, the Department of Homeland Security (DHS) has taken action to address a backlog of potential overstay records that GAO previously identified. Specifically, DHS reviewed such records to identify national security and public safety threats, but unmatched arrival records--those without corresponding departure records--remain in DHS's system. GAO had		

previously reported that, as of January 2011, DHS had a backlog of 1.6 million unmatched arrival records that had not been reviewed through automated or manual processes. DHS tracks arrivals and departures and closes records for individuals with matching arrival and departure records. Unmatched arrival records indicate that the individual is a potential overstay. In 2011, DHS reviewed this backlog of 1.6 million records, closed about 863,000 records, and removed them from the backlog. As new unmatched arrival records have accrued, DHS has continued to review all of these new records for national security and public safety concerns. As of June 2013, DHS's unmatched arrival records totaled more than 1 million. GAO recommends that DHS assess and document the reliability of its data, and establish time frames and milestones for a biometric air exit evaluation framework.

Mission 4: Safeguard and Secure Cyberspace

Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure

GAO Reports

Report: Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better defined and More Effectively Implemented	**Number:**	GAO-13-187
	Date:	2/14/2013

Summary: Threats to systems supporting critical infrastructure and federal operations are evolving and growing. Federal agencies have reported increasing numbers of cybersecurity incidents that have placed sensitive information at risk, with potentially serious impacts on federal and military operations; critical infrastructure; and the confidentiality, integrity, and availability of sensitive government, private sector, and personal information. The increasing risks are demonstrated by the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. The number of incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team has increased 782 percent from 2006 to 2012. GAO and inspector general reports have identified a number of key challenge areas in the federal government's approach to cybersecurity, including those related to protecting the nation's critical infrastructure. While actions have been taken to address aspects of these, issues remain in each of these challenge areas. To address missing elements in the national cybersecurity strategy, such as milestones and performance measures, cost and resources, roles and responsibilities, and linkage with other key strategy documents, GAO recommends that the White House Cybersecurity Coordinator develop an overarching federal cybersecurity strategy that includes all key elements of the desirable characteristics of a national strategy. Such a strategy would provide a more effective framework for implementing cybersecurity activities and better ensure that such activities will lead to progress in cybersecurity.

DHS OIG Reports

Report: DHS Can Make Improvements to Secure Industrial Control Systems	**Number:**	OIG-13-39
	Date:	2/14/13

Summary: NPPD has strengthened the security of ICS by addressing the need to share critical cybersecurity information, analyze vulnerabilities, verify emerging threats, and disseminate mitigation strategies. For example, DHS has taken the following actions to improve ICS security and foster better partnerships between the Federal and private sectors:

- Establishing ICS-CERT Incident Response Team, also known as the fly away teams, to support the public and private sectors through onsite and remote incident response services on a variety of cyber threats, ranging from general malicious code infections to advanced persistent threat intrusions. Additionally, in March 2012, NPPD released the Cyber Security Evaluation Tool Version 4.1. The updated tool assists users in identifying devices connected to their networks, as well as external connections, by creating a diagram of their systems.
- Operating a malware lab that provides testing capabilities to analyze vulnerabilities and malware threats to control system environments. The team verifies vulnerabilities for researchers and vendors, performs impact analysis, and provides patch validation and testing prior to deployment to the asset-owner community.
- Improving the quality of its alerts and bulletins by including actionable information

regarding vulnerabilities and recommended mitigations and best practices for securing ICS. • Providing products to the ICS community on a daily, weekly, monthly, quarterly, and as-needed basis, through email, website, and portal postings. These products help ICS-CERT to improve the situational awareness of ICS and provide status updates of its working groups, articles of interest, and upcoming events and training.

Testimony: Facilitating Cyber Threat Information Sharing and Partnering With The Private Sector To Protect Critical infrastructure: An Assessment of DHS Capabilities	**Number:**	Testimony
	Date:	5/16/2013
Summary: We reported that Department needed to improve the security of ICS and information sharing to enhance program effectiveness. DHS has strengthened the security of ICS by addressing the need to share critical cybersecurity information, analyze vulnerabilities, verify emerging threats, and disseminate mitigation strategies. For example, DHS has taken the following actions to improve ICS security and foster better partnerships between the Federal and private sectors.		

Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise

GAO Reports

Report: Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness	**Number:**	GAO-13-776
	Date:	9/26/2013
Summary: In fiscal year 2012, 24 major federal agencies had established many of the components of an information security program required by The Federal Information Security Management Act of 2002 (FISMA); however, they had partially established others. FISMA requires each federal agency to establish an information security program that incorporates eight key components, and each agency inspector general to annually evaluate and report on the information security program and practices of the agency. The act also requires the Office of Management and Budget (OMB) to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies and the National Institute of Standards and Technology to develop security standards and guidelines. The extent to which agencies implemented security program components showed mixed progress from fiscal year 2011 to fiscal year 2012. For example, according to inspectors general reports, the number of agencies that had analyzed, validated, and documented security incidents increased from 16 to 19, while the number able to track identified weaknesses declined from 20 to 15. GAO and inspectors general continue to identify weaknesses in elements of agencies' programs, such as the implementation of specific security controls. For instance, in fiscal year 2012, almost all (23 of 24) of the major federal agencies had weaknesses in the controls that are intended to limit or detect access to computer resources. OMB and the Department of Homeland Security (DHS) continued to develop reporting metrics and assist agencies in improving their information security programs; however, the metrics do not evaluate all FISMA requirements, such as conducting risk assessments and developing security plans; are focused mainly on compliance rather than effectiveness of controls; and in many cases did not identify specific performance targets for determining levels of implementation. Enhancements to these metrics would provide additional insight into agency information security programs.		

DHS OIG Reports		
Report: DHS Can Take Actions To Address Its Additional Cybersecurity Responsibilities	**Number:**	OIG-13-95
	Date:	6/5/2013
Summary: Despite these efforts, CS&C can take further actions to implement its additional cybersecurity responsibilities. For example, developing a strategic implementation plan and improving the communication and coordination with Federal agencies will help CS&C refine the FISMA reporting metrics and better evaluate agency information security programs. In addition, CS&C must establish a process to ensure that CyberScope contractor personnel receive adequate security training to perform their job functions. Finally, CS&C must configure CyberScope in accordance with DHS guidance.		

Mission 5: Strengthen National Preparedness and Resilience

Goal 5.1: Enhance National Preparedness

GAO Reports and Testimony

Report: Grants Performance: Justice and FEMA Collect Performance Data for Selected Grants, but Action Needed to Validate FEMA Performance Data	**Number:**	GAO-13-552
	Date:	6/24/2013

Summary: The Federal Emergency Management Administration's (FEMA) Emergency Management Performance Grants (EMPG) and Assistance to Firefighters Grants (AFG) programs collect performance information through a variety of reporting mechanisms. These mechanisms collect performance data used by FEMA regional offices and headquarters for different purposes. For example, headquarters focuses on the development of future program priorities and reporting progress toward the National Preparedness Goal, while regions use program information to monitor primary grant recipients. The Department of Homeland Security (DHS), of which FEMA is a part, developed agency priority goals that reflect agency-wide, near-term priorities. According to FEMA officials, the EMPG and AFG programs have an indirect link to a DHS agency priority goal, as well as the National Preparedness Goal, because they support states' level of preparedness for disasters. According to FEMA officials, neither program has a standardized tool with which to validate the performance data that are self-reported by recipients; additionally, the regions are inconsistent in their approaches to verifying program performance data. The absence of a formal established validation and verification procedure, as directed by Circular No. A-11, could lead to the collection of erroneous performance data. GAO recommends that FEMA ensure, in accordance with OMB Circular No. A-11, that there are consistent procedures in place at the program office and regional level to validate and verify grant performance data that allow FEMA to attest to the reliability of EMPG and AFG grant data used to report progress toward goals.

Testimony: National Preparedness: FEMA Has Made Progress, but Additional Steps Are Needed to Improve Grant Management and Assess Capabilities	**Number:**	GAO-13-637T
	Date:	6/25/2013

Summary: Officials in the Federal Emergency Management Agency (FEMA)--a component of the Department of Homeland Security (DHS)--have identified actions they believe will enhance management of the four preparedness programs GAO analyzed; however, FEMA still faces challenges. In February 2012, GAO found that FEMA lacked a process to coordinate application reviews and made award decisions with differing levels of information. To better identify potential unnecessary duplication, GAO recommended that FEMA collect project-level information and enhance internal coordination and administration of the programs. DHS concurred and has taken steps to address GAO's recommendations. For example, the fiscal year 2013 and 2014 President's budgets proposed the establishment of the National Preparedness Grant Program (NPGP), a consolidation of 16 FEMA grant programs into a single program. Members of Congress raised questions about the NPGP and did not approve the proposal for fiscal year 2013. FEMA incorporated stakeholder views, as directed by Congress, and the fiscal year 2014 President's Budget again proposed the NPGP. If approved, and depending on its final form and execution, the NPGP could help mitigate the potential for unnecessary duplication and address GAO's recommendation to improve internal coordination. In March 2013, FEMA officials reported that the agency intends to start collecting and analyzing project-level data from grantees in fiscal year 2014; but has not yet finalized data requirements or fully implemented the data system to collect the information. Collecting appropriate data and implementing project-level enhancements as planned would address GAO's recommendation and better position FEMA to

identify potentially unnecessary duplication.		
Report: National Capital Region Disaster Preparedness	**Number:**	GAO-13-116R
	Date:	1/31/2013
Summary: FEMA's NCRC officials are not assisting regional officials in (1) developing performance measures to better assess the implementation of their strategic plan and (2) identifying federal funding available to prioritize preparedness investments. They are not doing so because they view their role as that of acting as a coordinator for other federal agencies, although they agreed that they could do more to support regional efforts and are positioned to do so. The NCR Strategic Plan helps regional officials identify the capabilities needed to strengthen the region's homeland security efforts and defines the framework for achieving those capabilities. NCR preparedness officials said that they have been working to develop preparedness measures since 2003, but noted that these measures are difficult to link to a measured improvement in regional preparedness. For example, while the region identified more than $25 million in UASI grant projects invested in providing public alerts and warnings, regional officials have not developed a measure to determine the effectiveness of these activities. Without such measures, it is unclear to what extent the efforts will advance the region's goals. To address long-standing challenges that continue to hinder regional preparedness efforts in the NCR, we recommend that the FEMA Administrator require that the Director of NCRC take the following two actions: 1) assist regional officials in developing measures to better assess the implementation of the NCR's strategic plan; and 2) collect and maintain available information for NCR jurisdictions on DHS grant funding, and other federal grant funding that are relevant to homeland security and emergency management capabilities.		
Report: Nuclear Terrorism Response Plans: Major Cities Could Benefit From Federal Guidance on Responding to Nuclear and Radiological Attacks	**Number:**	GAO-13-736
	Date:	9/30/2013
Summary: Many emergency managers from the 27 major cities responding to GAO's questionnaire, although not all, reported that their city had assessed the risks of a terrorist attack using a radiological dispersal device (RDD) or improvised nuclear device (IND) and had ranked the risk of these attacks as lower than the risk of other hazards they face. GAO found limited federal planning guidance related to the early response capabilities needed by cities for the large RDD attack depicted in the national planning scenarios. Most cities that had RDD and IND response plans reported conducting exercises to validate the plans based on federal guidance. GAO recommends that FEMA develop guidance to clarify the early response capabilities needed by cities for RDD and IND attacks.		
DHS OIG Reports		
Testimony: Are We Prepared? Measuring The Impact of Preparedness Grants Since 9/11	**Number:**	Testimony
	Date:	6/25/2013
Summary: Through our FY 2013 and previous years' audits, we determined that in most instances the States complied with applicable laws and regulations in distributing and spending their awards. However, we noted several challenges related to the States' homeland security strategies, obligation of grants, reimbursement to subgrantees for expenditures, monitoring of subgrantees' performance and financial management, procurement, and property management.		
Testimony: Homeland Security Grants: Measuring Our Investments	**Number:**	Testimony
	Date:	3/19/2013
Summary: As a result of our audits, we have recommended that FEMA work with the States to improve HSGP management. FEMA concurred with almost all of our recommendations and has either coordinated with the State Administrative Agencies to implement them or taken steps to		

implement them. Although we audited the States' management of HSGP awards rather than FEMA's program management, we noted that FEMA could strengthen HSGP by issuing better guidance to the States on strategic planning, which would in turn improve the States' performance measurement and progress toward achieving their goals and objectives. For example, in our February 2013 report, *Kentucky's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded Fiscal Years 2008-2010*, we recommended that FEMA issue guidance to HSGP grantees to periodically update strategic plans and include goals that align with current National Preparedness Guidelines. According to officials in FEMA's Grant Programs Directorate, the National Preparedness Directorate was expected to issue updated guidance in the summer of 2013.

Goal 5.2: Mitigate Hazards and Vulnerabilities

GAO Reports

Report: Flood Insurance: Implications of Changing Coverage Limits and Expanding Coverage	**Number:**	GAO-13-568
	Date:	7/3/2013

Summary: The National Flood Insurance Program (NFIP) currently has more than 5.5 million policyholders insured for about $1.3 trillion who pay about $3.5 billion in annual premiums, but less than half purchase maximum coverage--a possible indicator of how many might purchase additional coverage were it offered. However, from 2002 through 2012, the proportion of residential and commercial policies at maximum building coverage rose substantially--from 11 to 42 percent and from 21 to 36 percent, respectively. States along the Gulf and East Coasts have the most residential policyholders with maximum coverage. In addition, states with higher median home values generally have a higher percentage of policyholders purchasing coverage up to the limit. Industry stakeholders said that an unknown number of policyholders with higher-value properties choose to purchase additional, or excess, coverage above the NFIP limit through the private flood insurance market--a small and selective group of insurers. Increasing coverage limits could increase the net revenue of the program and have varying effects on NFIP, the private insurance market, and consumers. Assuming that higher coverage limits had been in effect from 2002 through 2011, GAO's analysis suggests that NFIP still would have suffered losses during years with catastrophic floods, such as 2004 and 2005, but would have experienced net increases in revenue in other years. GAO continues to support previous recommendations to the Federal Emergency Management Agency (FEMA) that address the need to ensure that the methods and data used to set NFIP rates accurately reflect the risk of losses from flooding.

Report: Flood Insurance: More Information Needed on Subsidized Properties	**Number:**	GAO-13-607
	Date:	7/3/2013

Summary: The Biggert-Waters Flood Insurance Reform Act of 2012 (Biggert-Waters Act) immediately eliminated subsidies for about 438,000 National Flood Insurance Program (NFIP) policies, but subsidies on an estimated 715,000 policies across the nation remain. Depending on factors such as policyholder behavior, the number of subsidized policies will continue to decline over time. For example, as properties are sold and the Federal Emergency Management Agency (FEMA) resolves data limitations and defines key terms, more subsidies will be eliminated. GAO analysis found that remaining subsidized policies would cover properties in every state and territory where NFIP operates, with the highest numbers in Florida, Louisiana, and California. In comparing remaining subsidized and nonsubsidized policies GAO found varying characteristics. For example, counties with the highest and lower home values had a larger percentage of subsidized versus nonsubsidized policies. Data constraints limit FEMA's ability to estimate the aggregate cost of subsidies and establish rates reflecting actual flood risks on previously subsidized

policies. FEMA should develop and implement a plan to obtain flood risk information needed to determine full-risk rates for properties with previously subsidized rates.

Goal 5.3: Ensure Effective Emergency Response		
GAO Reports and Testimony		
Report: Emergency Alerting: Capabilities Have Improved, but Additional Guidance and Testing Are Needed	**Number:**	GAO-13-375
	Date:	5/23/2013
Summary: Since 2009, the Federal Emergency Management Agency (FEMA) has taken actions to improve the capabilities of the Integrated Public Alert and Warning System (IPAWS) and to increase federal, state, and local capabilities to alert the public, but barriers remain to fully implementing an integrated system. Specifically, IPAWS has the capability to receive and authenticate Internet-based alerts from federal, state, and local public authorities and disseminate them to the public through multiple systems. For example, since January 2012, public alerting authorities can disseminate Emergency Alert System (EAS) messages through IPAWS to television and radio stations. Beginning in April 2012, alerting authorities have used IPAWS to transmit alerts via the Commercial Mobile Alert System interface to disseminate text-like messages to mobile phones. FEMA also adopted alert standards and increased coordination efforts with multiple stakeholders. Although FEMA has taken important steps to advance an integrated system, state and local alerting authorities we contacted cited a need for more guidance from FEMA on how to integrate and test IPAWS capabilities with their existing alerting systems. For example, an official with a state alerting authority said that additional guidance from FEMA is needed to determine what systems and policies should be put in place before integrating and testing IPAWS with other public alerting systems in the state's 128 counties and cities. In the absence of sufficient guidance from FEMA, states we contacted are reluctant to fully implement IPAWS. This reluctance decreases the capability for an integrated, interoperable, and nationwide alerting system. GAO recommends that FEMA work in conjunction with FCC to establish guidance for states to fully implement and test IPAWS components and implement a strategy for regular nationwide EAS testing.		
Report: FEMA Reservists: Training Could Benefit from Examination of Practices at Other Agencies	**Number:**	GAO-13-250R
	Date:	4/22/2013
Summary: We compared FEMA's training of reservists with the training provided to reservists at the SBA, the Forest Service, and the Coast Guard--agencies with a disaster mission--and found similarities and differences; and, moreover, FEMA had not examined other agencies' training programs to identify useful practices. All four training programs shared some similar attributes with regard to training requirements, funding sources, training delivery, and training evaluation. For example, FEMA and two of the comparison agencies have a credentialing program used to document reservist qualifications. Differences included the timing of when training is delivered and the use of job aids to reinforce reservists' understanding of material covered in training courses. To enhance its training of reservists, we are recommending that FEMA examine the training practices of other agencies with disaster reservist workforces to identify potentially useful practices.		
DHS OIG Reports		
Report: DHS Needs to Manage Its Radio Communication Program Better	**Number:**	OIG-13-113
	Date:	8/29/2013

Summary: The Department of Homeland Security (DHS) operates and maintains 20 land mobile radio networks serving more than 120,000 frontline agents and officers. These users rely on radio systems for primary communications, officer safety, and mission success. DHS manages about 197,000 radio equipment items and 3,500 infrastructure sites, with a reported value of more than $1 billion. Many of these systems have exceeded their service-life and urgently need to be modernized to meet Federal and DHS mandates. DHS has estimated that full modernization of its existing end-of-life radio systems would require a $3.2 billion investment. The audit objective was to determine whether DHS is managing its radio program and related inventory in a cost-effective manner to prevent waste of taxpayer dollars. DHS is unable to make sound investment decisions for radio equipment and supporting infrastructure because the Department is not effectively managing its radio communication program. DHS does not have reliable Department-wide inventory data or an effective governance structure to guide investment decision-making. As a result, DHS risks wasting taxpayer funds on equipment purchases and radio system investments that are not needed, sustainable, supportable, or affordable. Two Components we visited stored more than 8,000 radio equipment items valued at $28 million for a year or longer at their maintenance and warehouse facilities, while some programs faced critical equipment shortages. Portfolio management is central to making informed decisions about how to best allocate available equipment to ensure the right equipment is in place at the right locations and in the quantities needed to conduct mission operations.		
Report: DHS' Oversight of Interoperable Communications	**Number:**	OIG-13-06
	Date:	11/2/2012
Summary: The Department of Homeland Security (DHS) includes an amalgamation of organizations that work together to prevent and respond to terrorist attacks, natural disasters, and other threats. Such collaboration requires that components establish effective communication among external and internal partners during operations. DHS established an internal goal of developing interoperable radio communications and identified common channels, and its components invested about $430 million in equipment, infrastructure, and maintenance to meet communication requirements. We performed this audit to determine whether DHS' oversight ensured achievement of Department-wide interoperable radio communications. DHS did not provide effective oversight to ensure that its components achieved Department-wide interoperable radio communications. It did not establish an effective governing structure that had the authority and responsibility to oversee its goal of achieving Department-wide interoperability. Without a governing structure, DHS had limited interoperability policies and procedures, and component personnel did not have interoperable radio communications. As a result, only 1 of 479 radio users tested could access and communicate using the specified common channel. Further, of the 382 radios tested, only 20 percent (78) contained all the correct program settings for the common channel. Until DHS develops an effective governing structure and makes a concerted effort to attain Department-wide interoperability, overall progress will remain limited.		
Report: FEMA Deployed the Appropriate Number of Community Relations Employees in Response to Hurricane Irene and Tropical Storm Lee	**Number:**	OIG-13-94
	Date:	5/31/2013

Summary: The number of DAEs deployed to perform community relations work in response to Hurricane Irene and Tropical Storm Lee was appropriate. FEMA generally managed the deployments in a manner consistent with achieving efficient JFO operations. We are not making any recommendations. FEMA deployed a reasonable number of DAEs to perform community relations work, given the disasters' magnitude and number of people affected. Specifically, FEMA deployed more than 800 DAEs to perform community relations work in response to Hurricane Irene and Tropical Storm Lee. This amount is well within FEMA's JFO staffing level targets and compares favorably with the total number of DAEs deployed in response to the disasters.		
Report: FEMA's Initial Response to Hurricane Isaac in Louisiana Was Effective and Efficient	**Number:**	OIG-13-84
	Date:	4/30/2013
Summary: Based on our observations, FEMA performed very well in its response to Hurricane Isaac. Normally, FEMA needs several days to deploy and position staff to the areas needed to respond to a disaster. In this case, FEMA was fortunate to have facilities and staff already operating in Louisiana when Hurricane Isaac made landfall. The ability to draw upon these resources allowed FEMA to respond faster and more effectively than usual. FEMA prepared well for this disaster, faced challenges with innovative solutions, quickly resolved resource shortfalls, made efficient disaster sourcing decisions, and coordinated its activities effectively with State and local officials. All disasters generate unexpected issues, but the FEMA disaster team was able to adjust and adapt quickly to fulfill its mission.		
Report: FEMA's Sheltering and Temporary Essential Power Pilot Program	**Number:**	OIG-13-15
	Date:	12/7/2012
Summary: FEMA established STEP pilot program, enabling residents to return to or remain in their homes as a form of shelter while permanent repairs are completed. FEMA's STEP pilot program is consistent with the authorities granted to the agency by the *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (Stafford Act) in assisting jurisdictions to perform activities that are essential in saving lives, protecting public health and safety, and protecting property. In carrying out this program, FEMA needs to address the vulnerabilities that are present whenever large sums of money are disbursed in a new and unique manner. The current situation requires increased vigilance to monitor the expenditure of public funds.		
Report: Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard	**Number:**	OIG-13-92
	Date:	5/23/2013
Summary: The USCG does not have adequate processes to investigate, take corrective actions, and enforce Federal regulations related to the reporting of marine accidents. These conditions exist because the USCG has not developed and retained sufficient personnel, established a complete process with dedicated resources to address corrective actions, and provided adequate training to personnel on enforcement of marine accident reporting. As a result, the USCG may be delayed in identifying the causes of accidents; initiating corrective actions; and providing the findings and lessons learned to mariners, the public, and other government entities. These conditions may also delay the development of new standards, which could prevent future accidents. We made seven recommendations to improve the efficiency and effectiveness of USCG's marine accident investigations and enforcement of reporting requirements. U SCG has concurred with all seven recommendations and is implementing corrective actions.		
Report: Federal Emergency Management Agency Needs To Improve Its Internal Controls Over the Use of Disaster Assistance Employees	**Number:**	OIG-13-13
	Date:	11/29/2013

Summary: FEMA paid approximately 1,600 individuals $36 million more than they would have received if FEMA had enforced its limitation of using DAEs no more than 18 months in a 2-year period ending September 30 of even-numbered years. FEMA made those payments in violation of FEMA Directive 8600.1 because it did not design the ADD system in a manner that allowed FEMA managers to systematically monitor the deployment period of DAEs. Thus, FEMA managers could not ensure that DAEs did not exceed the regulatory limit of 18 months of work in a 2-year period. In summary, 14 percent (1,600 of 11,000) of FEMA DAEs employed from October 2006 to September 2010 worked for longer than the 78 weeks allowed by policy.

A number of factors contributed to DAE deployments exceeding FEMA policy caps. Regional cadre managers at three FEMA regional offices said that, because of system limitations, they would have to take extraordinary and time-consuming steps to manage to a 78-week deployment limit. In addition, they said that mission considerations, such as the scarcity of skilled employees to fill certain roles and the overall disaster activity in a region, may necessitate the extension of certain DAEs beyond the deployment cap.

For example, if a person is one of a few in the cadre who has specific skills, or if a major disaster or several smaller disasters affect the region at once, a manager may have no choice other than deploying DAEs repeatedly in excess of the deployment cap. The extent to which DAEs were deployed in excess of 18 months in a 24-month period ranged from individuals who were deployed for an extra week or two to more than 400 individuals who were deployed for 26 weeks (6 months) to a year above the cap. The more notable examples of DAEs whose deployments exceeded the cap included a FEMA Region II DAE who was deployed full-time (208 weeks) during the entire 4-year period we examined, and a Region VII DAE who was deployed for 207 of 208 weeks during the period.

However, it does not appear that FEMA's noncompliance with Directive 8600.1 resulted in FEMA spending Disaster Assistance Fund appropriations on unnecessary work. In addition, contrary to the Office of Inspector General (OIG) Hotline complaint that was the origin of this report, we identified limited examples of employees whose deployment roles appeared to be positions of a continuous nature and not limited to a specific disaster, emergency, or project, as required by FEMA Directive 8600.1. However, those employees are being used to perform closeout activities on long-term public assistance and mitigation projects, not to perform nondisaster-related activities.

Goal 5.4: Enable Rapid Recovery

DHS OIG Reports

Report: Unless Modified, FEMA's Temporary Housing Plans Will Increase Costs by an Estimated $76 Million Annually	**Number:**	OIG-13-102
	Date:	1/10/2013

Summary: The Federal Emergency Management Agency (FEMA) announced a change in its temporary housing program that we estimate will increase costs and reduce efficiency and effectiveness. In 2012, FEMA announced that it would no longer use park models as a housing option, and instead would use only manufactured housing certified by the U.S. Department of Housing and Urban Development. Unless FEMA takes actions to ensure that it maintains the ability to use temporary housing units similar in size to the park model, this decision will increase program costs by tens of millions of dollars annually, and may hinder FEMA's ability to provide

shelter to disaster survivors quickly.

In reacting to the decision, FEMA field staff expressed concerns to us about their ability to house disaster survivors quickly and cost effectively. Further, FEMA officials said that many homeowners prefer units that can fit on their home sites, because it allows them to remain on their own property near their places of employment and schools while they rebuild their homes. Often, the larger manufactured housing units can be situated only on commercial sites, if available, or on FEMA-developed group sites. For 2011 disasters, 80 percent of units on private sites were park models. Based on our cost analysis, if FEMA placed manufactured housing units on group sites instead of park models on private sites, the increased cost of the temporary housing mission would be $76 million for a 12-month deployment. We question the decision to eliminate the park models. Since Hurricane Katrina, FEMA has improved the quality of its temporary housing units. FEMA resolved the unhealthy formaldehyde levels and the fire hazards related to the temporary housing units. A major contributing factor to improved housing conditions was FEMA's decision to discontinue the use of travel trailers, designed for recreational use, which were the source of many of the previous health and safety problems. Instead, FEMA provided survivors with manufactured housing units certified by the U.S. Department of Housing and Urban Development, along with smaller park models that are not certified. However, both of these deployed units still had various product quality, installation, and transportation issues. We have made one recommendation to improve the efficiency and effectiveness of the temporary housing unit program.

Mature and Strengthen Homeland Security

M&S.1: Integrate Intelligence, Information Sharing, and Operations

GAO Reports

Report: Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities	**Number:**	GAO-13-471
	Date:	4/4/2013

Summary: Five types of field-based information-sharing entities are supported, in part, by the federal government--Joint Terrorism Task Forces, Field Intelligence Groups, Regional Information Sharing Systems (RISS) centers, state and major urban area fusion centers, and High Intensity Drug Trafficking Area (HIDTA) Investigative Support Centers--and have distinct missions, roles, and responsibilities. However, GAO identified 91 instances of overlap in some analytical activities--such as producing intelligence reports--and 32 instances of overlap in investigative support activities, such as identifying links between criminal organizations. These entities conducted similar activities within the same mission area, such as counterterrorism, for similar customers, such as federal or state agencies. This can lead to benefits, such as the corroboration of information, but may also burden customers with redundant information. GAO also found that RISS centers and HIDTAs operate three different systems that duplicate the same function--identifying when different law enforcement entities may be conducting a similar enforcement action, such as a raid at the same location, to ensure officer safety--resulting in some inefficiencies. RISS and HIDTA have taken steps to connect two of the systems, but HIDTA does not have target time frames to connect the third system. A commitment to time frames would help reduce risks to officer safety and potentially lessen the burden on law enforcement agencies that are currently using multiple systems. Agencies have neither held entities accountable for coordinating nor assessed opportunities for further enhancing coordination to help reduce the potential for overlap and achieve efficiencies. The Departments of Justice (DOJ) and Homeland Security (DHS), and the Office of National Drug Control Policy (ONDCP)--the federal agencies that oversee or provide support to the five types of field-based entities-- acknowledged that entities working together and sharing information is important, but they do not hold the entities accountable for such coordination. GAO recommends that ONDCP work with HIDTA officials to establish time frames to connect systems; DHS, DOJ, and ONDCP develop measures to hold entities accountable for coordination and assess opportunities to enhance coordination; and the PM-ISE report on the results of the agencies' efforts to assess coordination.

DHS OIG Reports

Report: (U) Further Development and Reinforcement of Department Policies Can Strengthen DHS' Intelligence Systems Security Program	**Number:**	OIG-13-21
	Date:	1/10/2013

Summary: Since our fiscal year 2011 evaluation, the Office of Intelligence and Analysis (I&A) has improved its oversight of Department-wide systems and established programs to monitor ongoing security practices. I&A has developed and implemented a training program to educate DHS' growing number of personnel assigned security duties on intelligence systems. In addition, progress has been made in collaboration with other DHS components in centralizing the planning and prioritization of security weakness remediation, streamlining system configuration management, and maintaining a current systems inventory. However, we identified deficiencies at the United States Coast Guard (USCG) in system authorizations and specialized training and incident response, contingency planning, and security capital planning at the United States Secret Service (USSS). Also, we identified deficiencies in the Department-wide management of supply

chain threats and security capital planning. We made two recommendations to I&A, two recommendations to USCG, and three recommendations to USSS. DHS and its components concurred with all our recommendations. Fieldwork was conducted between April and July 2012.		
Report: DHS Uses Social Media To Enhance Information Sharing and Mission Operations, But Additional Oversight and Guidance Are Needed	**Number:**	OIG-13-115
	Date:	9/5/2013
Summary: DHS and its operational components have recognized the value of using social media to gain situational awareness and support mission operations, including law enforcement and intelligence-gathering efforts. However, additional oversight and guidance are needed to ensure that employees use technologies appropriately. In addition, improvements are needed for centralized oversight to ensure that leadership is aware of how social media are being used and for better coordination to share best practices. Until improvements are made, the Department is hindered in its ability to assess all the benefits and risks of using social media to support mission operations. We are recommending that the Department communicate the process to gain access to social media; establish a list of approved social media accounts used throughout the Department; complete the Department-wide social media policy to provide legal, privacy, and information security guidelines for the approved uses of social media; ensure that components develop and implement social media policies; and establish a forum for the Department and its components to collaborate and make decisions on the use of social media tools.		
Report: Homeland Security Information Network Improvements and Challenges	**Number:**	OIG-13-98
	Date:	1/12/2013
Summary: Since 2008, DHS has made progress in addressing the planning and governance issues we identified. Specifically, system program management performed an analysis of alternatives, revalidated stakeholder requirements, and developed other strategies to realign the program to address system challenges and concerns. Formalized governance processes established and supported by a new policy office contributed to these accomplishments. These efforts allowed the program to meet Office of Management and Budget requirements for program improvement, as well as acquisition review gateway criteria for the development of a new system release. Still, system program management has faced challenges implementing the new system release on schedule. Migration from the legacy system to the new platform has been delayed because of contracting and technical challenges. As a result, there is increased risk that schedule delays will lead to additional costs. Further, delays have caused some user communities to pursue other solutions for their information sharing needs. Although certain communities were using the system to share information successfully, the system was not routinely or widely used to share information throughout the homeland security enterprise. Specifically, the number of system account holders remained limited, and the extent to which those account holders were using the system was also constrained because of challenges with system content and performance. As a result, the system had not fully met its objective to support effective information sharing among homeland security partners.		

M&S.3: Conduct Homeland Security Research and Development		
GAO Reports and Testimony		
Report: Department of Homeland Security: Opportunities Exist to Better Evaluate and Coordinate Border and Maritime Research and Development	**Number:**	GAO-13-732
	Date:	9/25/2013
Summary: Between fiscal years 2010 and 2012, the Department of Homeland Security's (DHS) border and maritime research and development (R&D) components reported producing 97 R&D deliverables at an estimated cost of $177 million. The type of border and maritime R&D deliverables produced by DHS's Science and Technology (S&T) Directorate, the Coast Guard, and the Domestic Nuclear Detection Office (DNDO) varied, and R&D customers we met with reported mixed views on the impact of the R&D deliverables they received. These deliverables were wide-ranging in their cost and scale, and included knowledge products and reports, technology prototypes, and software (as shown in the figure below). The Coast Guard and DNDO reported having processes in place to collect and evaluate feedback from its customers regarding the results of R&D deliverables. However, S&T has not established timeframes and milestones for collecting and evaluating feedback from its customers on the extent to which the deliverables it provides to DHS components--such as US Customs and Border Protection (CBP)--are meeting its customer's needs. Doing so could help S&T better determine the usefulness and impact of its R&D projects and deliverables and make better-informed decisions regarding future work. GAO recommends that DHS S&T establish timeframes and milestones for collecting and evaluating feedback from its customers to determine the usefulness and impact of its R&D efforts, and ensure that potential challenges with regard to data reliability, accessibility, and availability are reviewed and understood before approving Centers of Excellence R&D projects.		
Testimony: Department of Homeland Security: Oversight and Coordination of Research and Development Efforts Could Be Strengthened	**Number:**	GAO-13-766T
	Date:	7/17/2013
Summary: In September 2012, GAO reported that the Department of Homeland Security (DHS) does not know the total amount its components invest in research and development (R&D) and does not have policies and guidance for defining R&D and overseeing R&D resources across the department. According to DHS, its Science & Technology Directorate (S&T), Domestic Nuclear Detection Office (DNDO), and U. S. Coast Guard (Coast Guard) are the only components that conduct R&D, and GAO found that these are the only components that report budget authority, obligations, or outlays for R&D activities to the Office of Management and Budget (OMB) as part of the budget process. However, GAO identified an additional $255 million in R&D obligations made by other DHS components. According to DHS, it is difficult to identify all R&D investments across the department because DHS does not have a department wide policy defining R&D or guidance directing components how to report all R&D spending and activities. As a result, it is difficult for DHS to oversee components' R&D efforts and align them with agency wide R&D goals and priorities. GAO recommended that DHS develop specific policies and guidance to assist DHS components in better understanding how to report R&D activities, and better position DHS to determine how much the agency invests in R&D to effectively oversee these investments.		
DHS OIG Reports		
Report: Research and Development Efforts To Secure Rail Transit Systems	**Number:**	OIG-13-111
	Date:	6/13/2013
Summary: The purpose of our review was to evaluate (1) how critical gaps in detecting improvised explosive device threats against mass transit systems are identified and prioritized for research and development, and (2) how S&T coordinates research and development efforts with		

TSA to address those gaps. The scope of this review was limited to the transportation sector's mass transit mode, specifically subway systems.

S&T and TSA replaced previously established working groups and processes with smaller, more effective groups, such as the Surface Transportation Project Integrated Product Team, chartered in 2010, and the Research and Development Working Group, reorganized in 2011. Although these groups and their associated processes are relatively new, they are successful in identifying and consolidating old and new capability gaps. In addition, S&T and TSA are effectively collaborating in research and development efforts to address mass transit security needs. Although the new gap analysis process is based on the Transportation Sector-Specific Security Plan, TSA does not have written guidelines or directives to formalize the process.

M&S.4: Train and Exercise Frontline Operators and First Responders		
GAO Reports		
Report: Border Security: U.S. Customs and Border Protection Has Taken Steps to Address GAO's Recommendations Aimed at Ensuring Officers are Fully Trained	**Number:**	GAO-13-768R
	Date:	8/28/2013
Summary: In December 2011, GAO reported that CBP had revised its training program for new CBP officers in accordance with training standards, but concluded that CBP could do more to identify and address incumbent officer training needs, such as evaluating the effectiveness of training and conducting a comprehensive assessment of the results of covert tests of CBP's inspection processes. For example, CBP developed and mandated training for all CBP officers in response to covert test results (e.g., a refresher course called "Back to Basics," and subsequent follow-on training), but it had not fully evaluated the effectiveness of the training. GAO made four recommendations to the CBP Commissioner. U.S. Customs and Border Protection (CBP) has taken actions to address the recommendations from GAO's December 2011 report on CBP officer training programs aimed at strengthening officer training; three of the four recommendations are closed, and CBP has actions underway to address the remaining open recommendation.		
Report: Border Security: U.S. Customs and Border Protection Provides Integrity-Related Training to Its Officers and Agents throughout Their Careers	**Number:**	GAO-13-769R
	Date:	8/28/2013
Summary: In December 2012, GAO reported on CBP's efforts to ensure the integrity of its workforce. For the purposes of that report, integrity issues included acts of corruption such as accepting cash bribes and other gratuities in return for allowing contraband or inadmissible aliens into the country, as well as other criminal activities or misconduct such as drug or alcohol abuse. GAO concluded that CBP had implemented integrity-related programs, but faced challenges in managing and overseeing these programs. In addition, GAO found that CBP had not completed an integrity strategy, as called for in its Fiscal Year 2009-2014 Strategic Plan. GAO recommended, among other things, that CBP set target timelines for completing and implementing a comprehensive integrity strategy to enhance CBP's efforts to mitigate the risk of corruption and misconduct among officers and agents. U.S. Customs and Border Protection's (CBP) integrity-related training courses are systematic and integrated--that is, they are offered in succession and required at each stage of an employee's career, as well as standardized and regularized--that is, the same content is provided by the same method on a predetermined, regular schedule. For example, courses are required throughout a CBP officer's and Border Patrol (BP) agent's career at the basic and supervisory levels, as well as on an annual basis.		

DHS OIG Reports		
Report: CBP Use of Force Training and Actions To Address Use of Force Incidents	**Number:**	OIG-13-114
	Date:	9/12/2013

Summary: CBP has taken several steps to address the number of use of force incidents involving CBP employees and to ensure that agents and officers use force only when necessary and reasonable. All CBP law enforcement agents and officers are required to follow the same use of force policy and standards and complete the same use of force training.

CBP tracks all use of force incidents and recently completed an internal review of use of force issues. However, more can be done. The CBP Office of Training and Development Use of Force Policy Division should incorporate additional assault data into its analysis of use of force incidents and formalize and expand its field audit program. CBP should continue to expand the use of scenario-based training and assess new technologies to support agents and officers.

M&S.5: Strengthen Service Delivery and Manage DHS Resources

GAO Reports and Testimony		
Testimony: Department of Homeland Security: Opportunities Exist to Strengthen Efficiency and Effectiveness, Achieve Cost Savings, and Improve Management Functions	**Number:**	GAO-13-547T
	Date:	4/26/2013

Summary: Since 2011, GAO has identified 11 areas across the Department of Homeland Security (DHS) where fragmentation, overlap, or potential duplication exists and 13 areas of opportunity for cost savings or enhanced revenue collections. In these reports, GAO has suggested 53 total actions to the department and Congress to help strengthen the efficiency and effectiveness of DHS operations. In GAO's 2013 annual report on federal programs, agencies, offices, and initiatives that have duplicative goals or activities, GAO identified 6 new areas where DHS could take actions to address fragmentation, overlap, or potential duplication or achieve significant cost savings. For example, GAO found that DHS does not have a department-wide policy defining research and development (R&D) or guidance directing components how to report R&D activities. Thus, DHS does not know its total annual investment in R&D, which limits its ability to oversee components' R&D efforts. In particular, GAO identified at least 6 components with R&D activities and an additional $255 million in R&D obligations in fiscal year 2011 by DHS components that was not centrally tracked. GAO suggested that DHS develop and implement policies and guidance for defining and overseeing R&D at the department. In addition, GAO reported that by reviewing the appropriateness of the federal cost share the Transportation Security Administration (TSA) applies to agreements financing airport facility modification projects related to the installation of checked baggage screening systems, TSA could, if a reduced cost share was deemed appropriate, achieve cost efficiencies of up to $300 million by 2030 and be positioned to install a greater number of optimal baggage screening systems. GAO has also updated its assessments of the progress that DHS and Congress have made in addressing the suggested actions from the 2011 and 2012 annual reports. As of March 2013, of the 42 actions from these reports, 5 have been addressed (12 percent), 24 have been partially addressed (57 percent), and the remaining 13 have not been addressed (31 percent). Although DHS and Congress have made some progress in addressing the issues that GAO has previously identified, additional steps are needed to address the remaining areas to achieve associated benefits.

Report: DHS Recruiting and Hiring: DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts	**Number:**	GAO-13-742
	Date:	9/17/2013
Summary: The Department of Homeland Security (DHS) and selected components are implementing strategies to fill mission-critical occupations (MCO), which are those occupations most critical to an agency's mission. In 2011, the Office of Diversity and Inclusion (D&I)--which coordinates component recruiting efforts--developed the Coordinated Recruiting and Outreach Strategy (CROS). Through the CROS, D&I intends to better coordinate and link component recruiting and outreach efforts to hiring for DHS mission and workforce needs (for all positions, including MCOs), and to leverage resources as well as reduce recruiting costs, among other things D&I has begun to implement the CROS through various means, including requiring components to develop their own outreach and recruiting plans that align with the CROS. However, D&I has been limited in its ability to implement some elements of the CROS--such as recruiter training--because of budget constraints, according to D&I officials. The components selected for GAO's review--the National Protection and Programs Directorate, Transportation Security Administration (TSA), U.S. Citizenship and Immigration Services, and U.S. Secret Service (USSS)--have also implemented various strategies to recruit and hire MCOs. In addition, these four components have generally been able to address hiring needs for MCOs. For example, USSS data show that vacancy rates were generally below 3 percent for MCO positions during fiscal years 2010 through 2012. Still, some officials have reported experiencing challenges attracting qualified candidates because of factors such as financial constraints and regional competition, among other things. For example, TSA has been challenged in filling certain positions in some areas where competition for other jobs makes it difficult to attract qualified candidates. GAO recommends that DHS require all components to provide recruiting cost information in a consistent manner.		
Report: DHS Strategic Workforce Planning: Oversight of Department-wide Efforts Should Be Strengthened	**Number:**	GAO-13-65
	Date:	12/3/2012
Summary: The Department of Homeland Security (DHS) has taken some relatively recent steps to enhance strategic workforce planning across the department. These steps are generally consistent with leading principles, but the department has not yet implemented an effective oversight approach for monitoring and evaluating components' progress. Specifically, recent steps DHS has taken to develop and implement strategic workforce planning efforts are consistent with the leading principles GAO has reported that include involving management and stakeholders, identifying skills and competencies, developing strategies to fill gaps, and building capability through training. For example, the department demonstrated stakeholder involvement by including component-level stakeholders in the development of the DHS Workforce Strategy. Though DHS has taken steps to implement strategic workforce planning, recent internal audits, as well as GAO's previous work, identified challenges related to workforce planning at the component level that could impair the continued implementation of recently initiated strategic workforce planning efforts. For example, GAO reported in July 2009 that the Federal Protective Service's (FPS) workforce planning was limited because FPS headquarters did not collect data on its workforce's knowledge, skills, and abilities and subsequently could not determine optimal staffing levels or determine how to modify its workforce planning strategies accordingly, amongst others. GAO recommends that, among other actions, the Secretary of Homeland Security (1) identify and document additional performance measures to assess workforce planning efforts and (2) document policies and procedures regarding the use of internal audit results.		

Testimony: Homeland Security: Observations on DHS's Oversight of Major Acquisitions and Efforts to Match Resources to Needs	**Number:**	GAO-13-846T
	Date:	9/19/2013
Summary: GAO has previously established that the Department of Homeland Security's (DHS) acquisition policy reflects many sound program management practices intended to mitigate the risks of cost growth and schedule slips. The policy largely reflects the knowledge-based approach used by leading commercial firms, which do not pursue major investments without demonstrating, at critical milestones, that their products are likely to meet cost, schedule, and performance objectives. DHS policy requires that important acquisition documents be in place and approved before programs are executed. For example, one key document is an acquisition program baseline, which outlines a program's expected cost, schedule, and the capabilities to be delivered to the end user. However, in September 2012, GAO found that the department did not implement the policy consistently, and that only 4 of 66 programs had all of the required documents approved in accordance with DHS's policy. GAO made five recommendations, which DHS concurred with, identifying actions DHS should take to mitigate the risk of poor acquisition outcomes and strengthen management activities. Further, GAO reported that the lack of reliable performance data hindered DHS and congressional oversight of the department's major programs. Officials explained that DHS's culture had emphasized the need to rapidly execute missions more than sound acquisition management practices. GAO also reported that most of the department's major programs cost more than expected, took longer to deploy than planned, or delivered less capability than promised. DHS has taken steps to improve acquisition management, but as part of its ongoing work, GAO found that DHS recently waived documentation requirements for 42 programs fielded for operational use since 2008. DHS explained it would be cost prohibitive and inefficient to recreate documentation for previous acquisition phases. GAO plans to obtain more information on this decision and its effect on the management of DHS's major acquisitions. DHS's July 2013 status assessment indicated that, as of the end of fiscal year 2012, many major programs still face cost and schedule shortfalls.		
Report: Information Technology: Agencies Need to Strengthen Oversight Of Billions Of Dollars In Operations and Maintenance	**Number:**	GAO-13-87
	Date:	11/15/2012
Summary: Federal agency assessments of the performance of information technology (IT) investments in operations and maintenance (O&M)--commonly referred to as operational analyses (OAs)--vary significantly. Office of Management and Budget (OMB) guidance calls for agencies to develop an OA policy and perform such analyses annually to ensure steady state investments continue to meet agency needs. The guidance also includes 17 key factors (addressing areas such as cost, schedule, customer satisfaction, and innovation) that are to be assessed. The five agencies GAO reviewed varied in the extent to which they carried out these tasks. The Departments of Homeland Security (DHS) and Health and Human Services (HHS) developed a policy which included all OMB assessment factors and performed OAs. However, they did not include all investments and key factors. In particular, DHS analyzed 16 of its 44 steady state investments, meaning 28 investments with annual budgets totaling $1 billion were not analyzed; HHS analyzed 7 of its 8 steady state investments. For OAs performed by DHS and HHS, both fully addressed approximately half of the key factors. With regard to the DHS and HHS investments that did not undergo an analysis or were not fully assessed against key factors, agency officials said this was due in part to program officials inconsistently applying OMB and agency guidance in conducting OAs and that OAs were not a priority. DHS and HHS have recently begun to take action to make OAs a priority and improve consistency. For example, DHS's chief information officer recently		

issued a directive requiring all steady state IT investments to conduct analyses annually and plans to assign staff in the office of the chief information officer to review them to ensure they are complete. GAO is recommending that DHS and HHS ensure OAs are being performed for all investments and that all factors are fully assessed.

Testimony: Information Technology: DHS Needs to Enhance Management of Major Investments	**Number:**	GAO-13-478T
	Date:	3/19/2013

Summary: Approximately two-thirds of the Department of Homeland Security's (DHS) major IT investments were meeting their cost and schedule commitments. Specifically, out of 68 major IT investments in development, 47 were meeting cost and schedule commitments. The remaining 21--which DHS had estimated to cost about $1 billion--had one or more subsidiary projects that were not meeting cost and/or schedule commitments (i.e., they exceeded their goals by at least 10 percent, which is the level at which the Office of Management and Budget (OMB) considers projects to be at increased risk of not being able to deliver planned capabilities on time and within budget.)

The primary causes for the cost and schedule shortfalls were (in descending order of frequency):

- inaccurate preliminary cost and schedule estimates,
- technical issues in the development phase,
- changes in agency priorities,
- lack of understanding of user requirements, and
- dependencies on other investments that had schedule shortfalls.

Eight of the investments had inaccurate cost and schedule estimates. For example, DHS's Critical Infrastructure Technology investment had a project where actual costs were about 16 percent over the estimated cost, due in part to project staff not fully validating cost estimates before proceeding with the project. In addition, six investments had technical issues in the development phase that caused cost or schedule slippages. For example, DHS's Land Border Integration investment had problems with wireless interference at certain sites during deployment of handheld devices used for scanning license plates, which caused a project to be more than 2 months' late.

DHS often did not adequately address cost and schedule shortfalls and their causes. GAO's investment management framework calls for agencies to develop and document corrective efforts to address underperforming investments and DHS policy requires documented corrective efforts when investments experience cost or schedule variances. Although 12 of the 21 investments with shortfalls had defined and documented corrective efforts, the remaining 9 had not. Officials responsible for 3 of the 9 investments said they took corrective efforts but were unable to provide plans or any other related documentation showing such action had been taken. Officials for the other 6 investments cited criteria in DHS's policy that excluded their investments from the requirement to document corrective efforts. This practice is inconsistent with the direction of OMB guidance and related best practices that stress developing and documenting corrective efforts to address problems in such circumstances. Until DHS addresses its guidance shortcomings and ensures each of these underperforming investments has defined and documented corrective efforts, these investments are at risk of continued cost and schedule shortfalls.

Report: Information Technology: Key Federal Agencies Need to Address Potentially Duplicative Investments	**Number:**	GAO-13-718
	Date:	9/12/2013

Summary: Of the 590 information technology (IT) investments reviewed, GAO identified 12 potentially duplicative investments at three key federal agencies--namely, the Departments of Homeland Security (DHS), Defense (DOD), and Health and Human Services (HHS). These investments accounted for about $321 million in reported IT spending for fiscal years 2008 through 2013. Of the 12 investments, GAO identified, two potentially duplicative investments [were] at DHS that support immigration enforcement booking management, which includes the processing of apprehended illegal aliens suspected of committing criminal violations of immigration law. DHS officials said having the two immigration booking investments were due in part to one component agency's unique requirements but were unable to provide analysis showing why one system could not satisfy the unique requirements. GAO recommends that DHS conduct analyses to address the potentially duplicative investments identified in this report.		
DHS OIG Reports		
Report: Department of Homeland Security's FY 2012 compliance with the Improper Payments Elimination and Recovery Act of 2010	**Number:**	OIG-13-47
	Date:	3/13/2013
Summary: We reviewed the accuracy and completeness of DHS' improper payment reporting and its efforts to reduce and recover improper payments. DHS needs to improve internal controls to ensure the accuracy and completeness of improper payment reporting. Specifically, it needs to improve its review processes to ensure that the risk assessments properly support the components' determination of programs susceptible to significant improper payments. Furthermore, DHS needs to adequately segregate duties and improve its policies and procedures to identify, reduce, and report improper payments.		
Testimony: DHS Acquisition Practices: Improving Outcomes For Taxpayers Using Defense And Private Sector Lessons Learned	**Number:**	Testimony
	Date:	9/19/2013
Summary: DHS needs a reliable department-wide inventory to help it plan, budget, schedule, and acquire upgrades and replacements of its radio systems and equipment. A department-wide inventory will help DHS prioritize its needs and plan its investments to make the most efficient use of available resources. It will also assist with planning for the acquisition and management of future communication networks. DHS also needs a strong governance structure over its radio communication program with adequate authority and resources to establish policy, make resource allocation and investment decisions, and hold Components accountable for managing radio programs and related inventories. A portfolio management approach to the DHS radio communication program would help ensure DHS receives a good return on investment when determining needs and allocating fiscal resources.		
Report: DHS Needs To Strengthen Information Technology Continuity and Contingency Planning Capabilities	**Number:**	OIG-13-110
	Date:	8/28/2013
Summary: Generally, DHS has made progress toward implementing effective disaster recovery capabilities at the Department's two enterprise data centers. Specifically, it has established a list of disaster recovery services that DHS components can procure for their systems. Additionally, the enterprise data centers now have disaster recovery enclaves that provide backup capabilities that allow continued minimum operations in the event of a disaster. Although DHS has strengthened its disaster recovery capabilities at the Enterprise Data Centers, more work is needed. For example, the Office of the Chief Information Officer's inadequate continuity and contingency planning increases the risk that the Department may not be able to respond effectively in case of an emergency or disaster. Specifically, the Department does not have a headquarters information		

technology disaster recovery plan that details the transition of its headquarters critical information systems and communication assets from the primary site to the alternate site. Also, the Office of the Chief Information Officer has not established policy that requires mission essential systems to be rated as having "high" criticality in accordance with the National Institute of Standards and Technology's Federal Information Processing Standards Publication 199. Finally, because of contingency planning weaknesses, all seven of the Department's enterprise mission essential systems that we reviewed are at risk of not having capabilities to react to emergency events, to restore essential business functions if a disruption occurs, and to resume normal operations.		
Report: FEMA's Efforts To Recoup Improper Payments in Accordance With the Disaster Assistance Recoupment Fairness Act of 2011 (6)	**Number:**	OIG-13-100
	Date:	6/21/2013
Summary: FEMA's effort to recoup improper payments in accordance with DARFA was cost effective. Congress passed the DARFA legislation in an attempt to mitigate the potentially unfair impact caused by the improper payments made by FEMA to individuals receiving disaster assistance subsequent to Hurricane Katrina and ending with disasters in December 2010. Congress could have drafted legislation that waived all such debt or created a process that provided FEMA the authority to waive the debt. Congress chose the latter. Because FEMA spent approximately $13.9 million on DARFA related activities and is scheduled to collect more than $15.2 million from debtors that did not meet DARFA requirements to receive a waiver, it was cost effective for FEMA to reevaluate the appropriateness of collecting the debt specified in the DARFA legislation. In addition, FEMA could collect an additional $281 million from debtors that never responded to Notice of Waiver letters significantly increasing cost effectiveness. Although FEMA's processing of DARFA cases was cost effective, FEMA did not adequately document about $58 million in potential improper payments it previously considered not warranted for recoupment. Specifically, FEMA determined that more than $225 million in potential debts did not warrant recoupment. However, FEMA could only provide potential debt amounts totaling about $167 million.		
Report: Major Management Challenges Facing the Department of Homeland Security (Revised)	**Number:**	OIG-13-09
	Date:	12/21/2012
Summary: 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.		
Testimony: DHS Information Technology: How Effectively Has DHS Harnessed IT To Secure Our Borders And Uphold Our Immigration Laws	**Number:**	Testimony
	Date:	3/19/2013

Summary: Components implementing transformation efforts are hindered by insufficient governance and decision-making mechanisms to effectively direct agency-wide transformation program activities. In our March 2011 report, we found that the USSS did not implement an effective IT governance approach for its Information Integration and Transformation Program, which had an estimated cost of $1.5 billion. Specifically, the agency did not have a formal department-level IT governance mechanism to provide integrated feedback and direction for the transformation program effort. Without a formal mechanism for integrated governance, the USSS reached out individually to DHS offices and received conflicting advice and did not sufficiently consider DHS enterprise-wide solutions. We recommended that the Deputy Director, USSS formalize an Executive Steering Committee and ensure that the Information Integration and Transformation Program is in alignment with the USSS and DHS strategic goals and objectives. Since that time, the USSS has provided updates on its ongoing efforts to implement an Executive Steering Committee which includes USSS Senior Management and DHS members from the offices of the CIO, the Chief Procurement Officer, and the Acquisition, Planning, and Management Directorate.		
Report: Evaluation of DHS' Information Security Program for Fiscal Year 2012	**Number:**	OIG-13-04
	Date:	10/24/2012
Summary: DHS continues to improve and strengthen its security program. During the past year, DHS developed and implemented the *Fiscal Year 2012 Information Security Performance Plan* to focus on areas that the Department would like to improve upon throughout the year. Specifically, DHS identified in the performance plan several key elements that are indicative of a strong security program, such as plans of action and milestones weakness remediation. In addition, DHS has taken actions to address the Administration's cybersecurity priorities, which include implementing trusted Internet connections, continuously monitoring DHS information systems, and employing personal identity verification compliant credentials to improve logical access for its systems. While these efforts have resulted in some improvements, components still are not executing all of the Department's policies, procedures, and practices. In addition, our review identified the following more significant exceptions to a strong and effective information security program: (1) systems are being authorized though key information is missing or outdated; (2) plans of action and milestones are not being created for all known information security weaknesses or mitigated in a timely manner; and (3) baseline security configurations are not being implemented for all systems. Additional information security program areas that need improvement include incident detection and analysis, specialized training, account and identity management, and contingency planning. Finally, the Department still needs to (1) consolidate all of its external connections, (2) implement a near-real-time monitoring capability, and (3) employ personal identity verification compliant cards for logical access on its information systems. We are making six recommendations to the Chief Information Security Officer. The Department concurred with all recommendations and has begun to take actions to implement them.		

Component Acronyms

Below is the list of DHS Components and their Acronyms.

AO – Analysis and Operations
CBP – U.S. Customs and Border Protection
DMO – Departmental Management and Operations
DNDO – Domestic Nuclear Detection Office
FEMA – Federal Emergency Management Agency
FLETC – Federal Law Enforcement Training Centers
ICE – U.S. Immigration and Customs Enforcement
NPPD – National Protection and Programs Directorate
OHA – Office of Health Affairs
OIG – Office of Inspector General
S&T – Science and Technology Directorate
TSA – Transportation Security Administration
USCG – U.S. Coast Guard
USCIS – U.S. Citizenship and Immigration Services
USSS – U.S. Secret Service

Homeland
Security

Homeland
Security