



# U.S. Department of Homeland Security Annual Performance Report

Fiscal Years 2015 – 2017

Appendix B: Program Evaluations



Homeland  
Security

# About this Report

---

The *U.S. Department of Homeland Security Annual Performance Report for Fiscal Years (FY) 2015-2017* presents the Department's performance measures and applicable results aligned to our missions, provides the planned performance targets for FY 2016 and FY 2017, and includes information on the Department's Strategic Review and our Agency Priority Goals. In addition, this report presents several FY 2015 Department-wide management initiatives followed by a summary of major management and performance challenges and high-risk areas identified by the DHS Office of Inspector General and the Government Accountability Office. The report is consolidated to incorporate our annual performance plan and annual performance report.

The *FY 2015 – 2017 Annual Performance Report* is one in a series of three reports which comprise the Department's performance and accountability reports:

- ***DHS Agency Financial Report:*** Delivery date – November 13, 2015.
- ***DHS Annual Performance Report:*** Delivery date – February 9, 2016.
- ***DHS Summary of Performance and Financial Information:*** Delivery date – February 16, 2016.

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](mailto:par@hq.dhs.gov) or calling (202) 447-0333.



Homeland  
Security



Visit Our Website  
[www.dhs.gov](http://www.dhs.gov)

## Table of Contents

Introduction .....	2
Mission 1: Prevent Terrorism and Enhance Security .....	3
Goal 1.1: Prevent Terrorist Attacks .....	3
Goal 1.2: Prevent and Protect Against the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities .....	7
Goal 1.3: Reduce Risk to the Nation’s Critical Infrastructure, Key Leadership, and Events .....	10
Mission 2: Secure and Manage Our Borders .....	12
Goal 2.1: Secure U.S. Air, Land, and Sea Borders and Approaches .....	12
Goal 2.2: Safeguard and Expedite Lawful Trade and Travel .....	17
Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors .....	20
Mission 3: Enforce and Administer Our Immigration Laws .....	22
Goal 3.1: Strengthen and Effectively Administer the Immigration System .....	22
Goal 3.2: Prevent Unlawful Immigration .....	25
Mission 4: Safeguard and Secure Cyberspace .....	30
Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure against Cyber Attacks and other Hazards .....	30
Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise .....	32
Goal 4.3: Advance Cyber Law Enforcement, Incident Response, and Reporting Capabilities .....	34
Goal 4.4: Strengthen the Cyber Ecosystem .....	34
Mission 5: Strengthen National Preparedness and Resilience .....	36
Goal 5.1: Enhance National Preparedness .....	36
Goal 5.2: Mitigate Hazards and Vulnerabilities .....	42
Goal 5.3: Ensure Effective Emergency Response .....	42
Goal 5.4: Enable Rapid Recovery .....	43
Mature and Strengthen Homeland Security .....	50
Goal: Integrate Intelligence, Information Sharing, and Operations .....	50
Goal: Enhance Partnerships and Outreach .....	50
Goal: Strengthen the DHS International Affairs Enterprise in Support of Homeland Security Missions .....	51
Goal: Conduct Homeland Security Research and Development .....	51
Goal: Ensure Readiness of Frontline Operators and First Responders .....	52
Goal: Strengthen Service Delivery and Manage DHS Resources .....	52
Component Acronyms .....	72

## 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 2015 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](http://www.gao.gov/browse/a-z/Department_of_Homeland_Security_Executive).

Detailed information on the findings and recommendations of FY 2015 DHS OIG reports is available at: [https://www.oig.dhs.gov/index.php?option=com\\_content&view=article&id=217&Itemid=206](https://www.oig.dhs.gov/index.php?option=com_content&view=article&id=217&Itemid=206).

# Mission 1: Prevent Terrorism and Enhance Security

## Goal 1.1: Prevent Terrorist Attacks

### GAO Reports

#### **Aviation Security: TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed**

**Number:** [GAO-15-678T](#)

**Date:** 6/9/2015

**Summary:** The Transportation Security Administration (TSA) has taken steps to improve oversight of Secure Flight—a passenger prescreening program that matches passenger information against watch lists to assign each passenger a risk category—but could take further action to address screening errors. In September 2014, GAO reported that TSA lacked timely and reliable information on system matching errors—instances where Secure Flight did not identify passengers who were actual matches to watch lists. GAO recommended that TSA systematically document such errors to help TSA determine if actions can be taken to prevent similar errors from occurring. The Department of Homeland Security (DHS) concurred and has developed a mechanism to do so, but has not yet shown how it will use this information to improve system performance. In September 2014, GAO also found that screening personnel made errors in screening passengers at the checkpoint at a level consistent with their Secure Flight risk determinations and that TSA did not have a systematic process for evaluating the root causes of these errors across airports. GAO recommended that TSA develop a process for evaluating the root causes and implement corrective measures to address them. DHS concurred and has developed such a process but has not yet demonstrated implementation of corrective measures.

In March 2014, GAO found that TSA performance assessments of certain full-body scanners used to screen passengers at airports did not account for all factors affecting the systems. GAO reported that the effectiveness of Advanced Imaging Technology (AIT) systems equipped with automated target recognition software (AIT-ATR)—which displays anomalies on a generic passenger outline instead of actual passenger bodies—relied on both the technology's capability to identify potential threat items and its operators' ability to resolve them. However, GAO found that TSA did not include these factors in determining overall AIT-ATR system performance. GAO also found that TSA evaluated the technology's performance in the laboratory—a practice that does not reflect how well the technology will perform with actual human operators. In considering procurement of the next generation of AIT systems (AIT-2), GAO recommended that TSA measure system effectiveness based on the performance of both the technology and the screening personnel. DHS concurred and in January 2015 reported that it has evaluated the AIT-2 technology and screening personnel as a system but has not yet provided sufficient documentation of this effort.

In December 2014, GAO found that TSA had not tested the effectiveness of its overall Managed Inclusion process—a process to assess passenger risk in real time at the airport and provide expedited screening to certain passengers—but had plans to do so. Specifically, GAO found that TSA had tested the effectiveness of individual components of the Managed Inclusion process, such as canine teams, but had not yet tested the effectiveness of the overall process. TSA officials stated

that they had plans to conduct such testing. Given that GAO has previously reported on TSA challenges testing the effectiveness of its security programs, GAO recommended that TSA ensure its planned testing of the Managed Inclusion process adhere to established evaluation design practices. DHS concurred and has plans to use a test and evaluation process for its planned testing of Managed Inclusion.

### **Aviation Security: TSA Has Taken Steps to Improve Vetting of Airport Workers**

**Number:** [GAO-15-704T](#)

**Date:** 6/16/2015

**Summary:** The Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), requires that before airport operators issue credentials to applicants seeking unescorted access to secure areas of an airport, the applicant must be vetted in accordance with TSA requirements, which generally includes a Security Threat Assessment. GAO reported in December 2011 that this assessment includes checks of criminal history records and immigration status, as well as a check against terrorist databases. To initiate the Security Threat Assessment, airport operators collect applicant information and transmit the results to TSA. TSA adjudicates the immigration and terrorism checks, initiates an automated check of Federal Bureau of Investigation (FBI) criminal history records, and transmits the results of the criminal history record checks to the airport operators. The airport operators are responsible for adjudicating the criminal history to identify potentially disqualifying criminal offenses specified under TSA regulations, and making a final determination of eligibility for a credential.

TSA has taken steps to ensure that airport workers who require unescorted access to secure areas of commercial (i.e., TSA-regulated) airports are properly vetted to ensure they do not pose a security threat. However, GAO previously found that TSA faced challenges in ensuring it had the necessary criminal information to effectively conduct Security Threat Assessments for aviation workers. In December 2011, GAO found that limitations in TSA's criminal history checks increased the risk that the agency was not detecting potentially disqualifying criminal offenses as part of its Security Threat Assessments for airport workers. TSA reported that its ability to review applicant criminal history records was often incomplete due to its status as a noncriminal justice agency. GAO found that TSA and FBI had not assessed whether a potential security risk in TSA's Security Threat Assessment process could exist as a result. As a result, GAO recommended that the TSA and the FBI jointly assess the extent to which this limitation may pose a security risk, identify alternatives to address any risks, and assess the costs and benefits of pursuing each alternative. TSA and the FBI have since taken steps to address this recommendation. As of September 2014, TSA officials reported that the FBI has taken steps to expand the criminal history record information available to TSA when conducting its Security Threat Assessments for airport workers and others. In April 2015, the Secretary of DHS stated that until TSA establishes a system for "real-time recurrent" criminal history records checks for all airport workers beyond their time of initial employment, the agency shall require fingerprint-based criminal history records checks every two years for such workers with unescorted access to secure areas of the airport. TSA subsequently updated existing requirements to implement procedures consistent with the Secretary's statement.

**DHS OIG Reports****Security Enhancements Needed to the TSA PreCheck® Initiative****Number:** [OIG-15-29](#)**Date:** 1/28/2015

**Summary:** In November 2001, Congress authorized TSA to implement trusted passenger programs to expedite security screening of participating passengers. The intent is to allow airport security personnel the ability to focus more extensive screening on higher-risk and unknown populations. In response, TSA introduced the TSA Pre✓® initiative in October 2011. TSA identified low-risk passengers to receive expedited screening through TSA Pre✓® lanes at airport security checkpoints. Our objectives were to determine what processes and procedures exist to ensure proper vetting of applicants, how TSA assesses member continued eligibility, and how TSA tests its processes for not effectively target and examine rail shipments effectiveness and timeliness. We made recommendations to assist TSA in correcting deficiencies to meet its expedited screening goals. In addition to an unclassified summary, we issued to the Department and Congress a Classified and a Sensitive Security Information version of this report.

**Allegation of Granting Expedited Screening through TSA PreCheck Improperly (Redacted)****Number:** [OIG-15-45](#)**Date:** 3/16/2015

**Summary:** OSC received a whistleblower disclosure alleging a notorious convicted felon was improperly cleared for TSA Pre✓® screening, creating a significant aviation security breach. The disclosure identified this event as a possible error in the TSA Secure Flight program since the traveler's boarding pass contained a TSA Pre✓® indicator and encrypted bar code. The investigation objectives were to determine whether a convicted felon was improperly granted expedited screening through Pre✓® despite having disqualifying criminal convictions, and whether the event indicates a possible error in the program. It was determined that TSA did not grant the traveler TSA Pre✓® screening through the TSA Pre✓® Application Program or managed inclusion. TSA granted the traveler TSA Pre✓ screening through risk assessment rules in the Secure Flight program. We made two recommendations aimed at improving the TSA Pre✓® Initiative security. TSA concurred with one recommendation and did not concur with the other. In addition to the redacted report, we issued a Sensitive Security Information version to the Department and Congress.

**The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program****Number:** [OIG-15-86](#)**Date:** 5/6/2015

**Summary:** TSA is not properly managing the maintenance of its airport screening equipment. Specifically, TSA has not issued adequate policies and procedures to airports for carrying out equipment maintenance-related responsibilities. Because TSA does not adequately oversee equipment maintenance, it cannot be assured that routine preventive maintenance is performed or that equipment is repaired and ready for operational use.

Without diligent oversight, including implementing adequate policies and procedures and ensuring it has complete, accurate, and timely maintenance data for thousands of screening equipment units, TSA risks shortening equipment life and incurring costs to replace equipment. If the equipment is not fully operational, TSA may have to use other screening measures, which could result in longer wait times and delays in passenger and baggage screening. More importantly, our prior work on airport passenger and baggage screening demonstrated that these other measures may be less effective at detecting dangerous items. Consequently, the safety of airline passengers and aircraft could be jeopardized.

### **TSA Can Improve Aviation Worker Vetting (Redacted)**

**Number:** [OIG-15-98](#)

**Date:** 6/4/2015

**Summary:** TSA's multi-layered process to vet aviation workers for potential links to terrorism was generally effective. In addition to initially vetting every application for new credentials, TSA recurrently vetted aviation workers with access to secured areas of commercial airports every time the Consolidated Terrorist Watchlist was updated. However, our testing showed that TSA did not identify 73 individuals with terrorism-related category codes because TSA is not authorized to receive all terrorism-related information under current interagency watchlisting policy.

TSA had less effective controls in place for ensuring that aviation workers 1) had not committed crimes that would disqualify them from having unescorted access to secure airport areas and 2) had lawful status and were authorized to work in the United States. In general, TSA relied on airport operators to perform criminal history and work authorization checks, but had limited oversight over these commercial entities. Thus, TSA lacked assurance that it properly vetted all credential applicants.

Further, thousands of records used for vetting workers contained potentially incomplete or inaccurate data, such as an initial for a first name and missing social security numbers. TSA did not have appropriate edit checks in place to reject such records from vetting. Without complete and accurate information, TSA risks credentialing and providing unescorted access to secure airport areas for workers with potential to harm the nation's air transportation system.

### **Use of Risk Assessment within Secure Flight (Redacted)**

**Number:** [OIG-14-153](#)

**Date:** 6/15/2015

**Summary:** The U.S. Office of Special Counsel (OSC) received a whistleblower disclosure concerning the use of a risk-based rule by the Transportation Security Administration's (TSA) Secure Flight program that may create a vulnerability in aviation security related to the risk-based rule. On April 28, 2014 OSC referred the allegation to the Secretary of DHS. DHS then requested OIG assistance with the allegation. TSA mitigated risk with this rule by suspending the rule's use in the Secure Flight program on March 7, 2014.

## **Covert Testing of TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints**

**Number:** [OIG-15-150](#)

**Date:** 9/22/2015

**Summary:** The Transportation Security Administration (TSA) conducts or oversees passenger checkpoint screening at 450 federalized airports. Passenger checkpoint screening is a process by which passengers are inspected to deter, detect, and prevent explosives, incendiaries, weapons, or other security threats from entering sterile areas of an airport or getting onboard an aircraft. As threats to transportation security evolved, TSA needed a screening technology to detect nonmetallic threats. TSA developed Advanced Imaging Technology (AIT) to screen passengers for both metallic and nonmetallic threats concealed under clothing—without physical contact. In 2013, TSA equipped all AIT with Automated Target Recognition software, which displays a box around anomalies on a generic outline of a body.

Our objective was to determine the effectiveness of TSA's AIT, Automated Target Recognition software, and checkpoint screener performance in identifying and resolving anomalies and potential security threats at airport checkpoints. The compilation of the number of tests conducted, names of the test airports, and quantitative and qualitative results of our testing is classified or designated as Sensitive Security Information. We have shared the information with the Department, TSA, and appropriate Congressional committees.

We made one recommendation that when implemented should strengthen the effectiveness of identifying and resolving security threats at airport checkpoints.

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

### **GAO Reports**

#### **Biosurveillance: Additional Planning, Oversight, and Coordination Needed to Enhance National Capability**

**Number:** [GAO-15-664T](#)

**Date:** 7/8/2015

**Summary:** In June 2010, GAO reported that there was neither a comprehensive national strategy nor a designated focal point with the authority and resources to guide development of a national biosurveillance capability. Further, in October 2011, GAO reported that states and local agencies faced challenges in developing and maintaining their biosurveillance capabilities, such as obtaining resources for an adequate workforce, and that the federal government had not conducted an assessment of state and local jurisdictions' ability to contribute to a national biosurveillance capability. To help ensure the successful implementation of a complex, intergovernmental undertaking, GAO recommended in 2010 that the White House's Homeland Security Council direct the National Security Council Staff to develop a national biosurveillance strategy, and further recommended in 2011 that the strategy consider nonfederal capabilities. The White House issued

the National Strategy for Biosurveillance in July 2012, which describes the U.S. government's approach to strengthening biosurveillance. However, the strategy did not fully respond to the challenges GAO identified. For example, it did not establish a framework to prioritize resource investments or address the need to leverage nonfederal resources. The White House was to issue an implementation plan within 120 days of publishing the strategy. GAO has reported that it is possible that the implementation plan could address issues previously identified, such as resource investment prioritization; however, the plan has not been released as of June 2015.

In August 2011, GAO reported that there was no centralized coordination to oversee federal agencies' efforts to implement Homeland Security Presidential Directive 9 (HSPD-9) on the nation's food and agriculture defense policy, which includes food and agriculture disease surveillance. GAO also found that the Department of Agriculture (USDA) had no department-wide strategy for implementing its HSPD-9 responsibilities. Therefore, GAO recommended that the National Security Council Staff and the Department of Homeland Security resume their efforts to coordinate and oversee implementation, and that USDA develop a department-wide strategy. In response, the National Security Council Staff began hosting interagency working group meetings, and DHS has worked to develop a report on agencies' HSPD-9 implementation efforts, which officials stated will be finalized by late summer 2015. As of February 2015, USDA had conducted a gap analysis of its HSPD-9 implementation efforts but had not yet developed a department-wide strategy. Further, GAO reported in May 2013 that USDA's Animal and Plant Inspection Service (APHIS) had broadened its previous disease-by-disease surveillance approach to an approach in which the agency monitors the overall health of livestock and poultry, but had not yet integrated this approach into an overall strategy aligned with the nation's larger biosurveillance efforts, such as efforts called for in HSPD-9. GAO recommended that APHIS integrate its new approach into an overall strategy aligned with national homeland security efforts, and develop goals and measures for the new approach. In June 2015, officials stated that APHIS has begun to develop some measures, but noted that resource constraints limit their ability to assess their new approach to disease surveillance. Fully integrating its new approach into an overall strategy aligned with broader homeland security efforts, as GAO recommended, will better position APHIS to support national efforts to address threats to animal and human health.

### **Critical Infrastructure Protection: DHS Action Needed to Verify Some Chemical Facility Information and Manage Compliance Process**

**Number:** [GAO-15-614](#)

**Date:** 7/22/2015

**Summary:** Since 2007, the Office of Infrastructure Protection's Infrastructure Security Compliance Division (ISCD), within the Department of Homeland Security (DHS), has identified and collected data from approximately 37,000 chemical facilities under its Chemical Facility Anti-Terrorism Standards (CFATS) program and categorized approximately 2,900 as high-risk based on the collected data. However, ISCD used unverified and self-reported data to categorize the risk level for facilities evaluated for a toxic release threat. A toxic release threat exists where chemicals, if released, could harm surrounding populations. One key input for determining a facility's toxic release threat is the Distance of Concern (distance) that facilities report—an area in which exposure to a toxic chemical cloud could cause serious injury or fatalities from short-term exposure. ISCD requires facilities to calculate the distance using a web-based tool and following DHS guidance. ISCD does not verify facility-reported data for facilities it does not categorize as high-risk for a toxic release threat. However, following DHS guidance and using a generalizable sample of

facility-reported data in a DHS database, GAO estimated that more than 2,700 facilities (44 percent) of an estimated 6,400 facilities with a toxic release threat misreported the distance. By verifying that the data ISCD used in its risk assessment are accurate, ISCD could better ensure it has identified the nation's high-risk chemical facilities.

ISCD has made substantial progress approving site security plans but does not have documented processes and procedures for managing facilities that are noncompliant with their approved site security plans. Site security plans outline, among other things, the planned measures that facilities agree to implement to address security vulnerabilities. As of April 2015, GAO estimates that it could take between 9 and 12 months for ISCD to review and approve security plans for approximately 900 remaining facilities—a substantial improvement over the previous estimate of 7 to 9 years GAO reported in April 2013. ISCD officials attributed the increased approval rate to efficiencies in ISCD's security plan review process, updated guidance, and a new case management system. Further, ISCD began conducting compliance inspections in September 2013, but does not have documented processes and procedures for managing the compliance of facilities that have not implemented planned measures outlined in their site security plans. According to the nature of violations thus far, ISCD has addressed noncompliance on a case-by-case basis. Almost half (34 of 69) of facilities ISCD inspected as of February 2015 had not implemented one or more planned measures by deadlines specified in their approved site security plans and therefore were not fully compliant with their plans. GAO found variations in how ISCD addressed these 34 facilities, such as how much additional time the facilities had to come into compliance and whether or not a follow-on inspection was scheduled. Such variations may or may not be appropriate given ISCD's case-by-case approach, but having documented processes and procedures would ensure that ISCD has guidelines by which to manage noncompliant facilities and ensure they close security gaps in a timely manner. Additionally, given that ISCD will need to inspect about 2,900 facilities in the future, having documented processes and procedures could provide ISCD more reasonable assurance that facilities implement planned measures and address security gaps.

### **Biosurveillance: Challenges and Options for the National Biosurveillance Integration Center**

**Number:** [GAO-15-793](#)

**Date:** 9/24/2015

**Summary:** The National Biosurveillance Integration Center (NBIC) has activities that support its integration mission, but faces challenges that limit its ability to enhance the national biosurveillance capability. In the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) and NBIC Strategic Plan, GAO identified three roles that NBIC must fulfill to meet its biosurveillance integration mission. The following describes actions and challenges in each role:

- **Analyzer:** NBIC is to use technology and subject matter expertise, including using analytical tools, to meaningfully connect disparate datasets and information for earlier warning and better situational awareness of biological events. GAO found that NBIC produces reports on biological events using open-source data, but faces challenges obtaining data and creating meaningful new information. For example, most of the federal partners with key roles in biosurveillance (8 of 11) stated that NBIC's products help their agencies identify biological events to little or no extent, generally because they already obtain such information directly from other federal partners more quickly. In addition, data that could help to identify and characterize a biological event may not exist or are not in a usable form. Further, few

federal partners (5 of 19) reported that they share the data they do have with NBIC, citing legal and regulatory restrictions, among other reasons.

- **Coordinator:** NBIC is to bring together partners across the federal biosurveillance community to enhance understanding of biological events. NBIC has developed procedures and activities to coordinate with partners, such as daily and biweekly calls, but faces challenges related to the limited partner participation in the center's activities, lack of partner personnel detailed to NBIC, and competing structures for convening federal partners. For example, although NBIC would like to obtain liaisons from each of its federal partners, only 3 of 19 partners provided NBIC with dedicated liaisons.
- **Innovator:** NBIC is to facilitate the development of new tools to address gaps in biosurveillance integration. GAO found that NBIC has efforts underway to develop some tools, such as pilot projects examining the use of social media data to identify health trends, but faces challenges prioritizing developmental efforts. For example, partners noted limitations in NBIC's ability to address gaps, like limited resources and the difficulty in prioritizing the center's innovation efforts because its partners have diverse needs.

GAO identified various options that could address these challenges, ranging from strengthening the center's ability to implement its current roles to repealing NBIC's statute. GAO also identified potential benefits and limitations with each option. For example, one option would be to provide NBIC with additional authorities to obtain data to better develop meaningful information; however this may also require additional investments. Another option is to not pursue national biosurveillance integration through NBIC and to consider designating one of the other federal partners with key roles in biosurveillance as the federal integrator. The options identified are not exhaustive, and some could be implemented together or in part. GAO did not evaluate the financial implications of each option, but acknowledges some options may require additional investment or shifting of resources or priorities to result in significant long lasting change.

### DHS OIG Reports

No OIG reports were available that aligned to this goal.

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

### GAO Reports

No OIG reports were available that aligned to this goal.

**DHS OIG Reports****Management Advisory-Alarm System Maintenance at Residences Protected by the U.S. Secret Service (Redacted)****Number:** [OIG-15-61](#)**Date:** 4/20/2015

**Summary:** In October 2014, OIG visited former President George H.W. Bush's Houston residence in response to a complaint alleging alarms were inoperable. During our visit, we identified issues with the alarm system at the residence. Specifically, we determined the alarm had been inoperable for at least 13 months. During this time, the Secret Service protective detail created a roving post to secure the residence and no security breach occurred. However, we found problems with identifying, reporting, and tracking alarm system malfunctions, and with repairing and replacing alarm systems. OIG informed secret service as the issues may be affecting other residences. OIG made two recommendations aimed at identifying existing inoperable security equipment at protectee's residences and improving processes for resolving security equipment problems at protectee's residences.

## Mission 2: Secure and Manage Our Borders

### Goal 2.1: Secure U.S. Air, Land, and Sea Borders and Approaches

#### GAO Reports

##### **Border Security: Additional Efforts Needed to Address Persistent Challenges in Achieving Radio Interoperability**

**Number:** [GAO-15-201](#)

**Date:** March 23, 2015

**Summary:** GAO was asked to evaluate DHS border security and immigration tactical communications (TACCOM) programs and operational impacts resulting from interoperability challenges. This report addresses the extent to which (1) U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) have upgraded tactical communications equipment and infrastructure along the U.S. southwest border, (2) CBP and ICE have provided tactical communications training to radio users, and (3) DHS has taken actions to improve the interoperability of tactical communications along the U.S. southwest border and what challenges, if any, remain.

GAO found that CBP and ICE have taken steps to upgrade tactical communications equipment and infrastructure, but could benefit by developing performance and program plans. GAO recommends that CBP and ICE develop performance and program plans for their modernization programs, mechanisms to track training, and plans to address skills gaps in understanding radio systems.

##### **Border Security: Progress and Challenges in DHS's Efforts to Implement and Assess Infrastructure and Technology**

**Number:** [GAO-15-595T](#)

**Date:** May 13, 2015

**Summary:** GAO reported in March 2014 that U.S. Customs and Border Protection (CBP) had made progress in deploying programs under the Arizona Border Surveillance Technology Plan (the Plan), but that CBP could strengthen its management and assessment of the Plan's programs. In March 2014, GAO reported that while CBP had identified mission benefits of technologies to be deployed under the Plan, such as improved situational awareness, the agency had not developed key attributes for performance metrics for all technologies, as GAO recommended. In April 2015, GAO reported that CBP had identified a set of potential key attributes for performance metrics for deployed technologies and CBP officials stated that by the end of fiscal year 2015, baselines for each performance measure will be developed and the agency will begin using the data to evaluate the contributions of specific technology assets.

In March 2015, GAO reported that DHS, CBP, and U.S. Immigration and Customs Enforcement (ICE) had taken steps to upgrade tactical communications equipment and infrastructure, such as completing full modernization projects in four of the nine southwest border sectors, but could benefit by developing performance and program plans. Since rolling out upgrades CBP had not established an ongoing performance monitoring plan to determine whether the systems were

working as intended. Further, GAO reported in March 2015 that ICE did not have a program plan to manage its portfolio of modernization projects.

In March 2012, GAO reported that the Office of Air and Marine (OAM) within CBP could benefit from reassessing its mix and placement of assets to better address mission needs and threats. GAO reported that OAM should clearly document the linkage of deployment decisions to mission needs and threat and its analysis and assessments used to support its decisions on the mix and placement of assets. GAO also reported that OAM could consider how border technology deployment will affect customer requirements for OAM assets. GAO recommended that CBP reassess the mix and placement of OAM's assets to include mission requirements, among other things.

## DHS OIG Reports

### Evaluation of Alleged AUO Misuse at U.S. Border Patrol, Ysleta Station

**Number:** [DI-14-0631](#)

**Date:** November 04, 2014

**Summary:** The U.S. Officer of Special Counsel (OSC) received a whistleblower disclosure concerning U.S. Customs and Border Protection's Ysleta Border Patrol Station in El Paso, Texas alleging that supervisors and border patrol agents claim administratively uncontrollable overtime (AUO), but fail to perform duties that qualify AUO. The whistleblower also alleged that supervisors authorize AUO to compensate injured agents who are assigned administrative duties and are not working overtime hours. OIG assembled a taskforce to review these allegations.

The taskforce found that the Ysleta Station did not have sufficient AUO documentation to allow the taskforce to specifically identify a violation of law, rule, or regulation. However, most activities that second-line supervisory border patrol agents perform appear to have been administratively controllable. OIG did not find evidence to substantiate that Ysleta Station agents who sustained work-related injuries were paid AUO improperly. This report contains no recommendations.

### Evaluations of Alleged AUO Misuse at U.S. Customs and Border Protection's National Targeting Center

**Number:** [DI-14-0581](#)

**Date:** Dec 02, 2014

**Summary:** The U.S. Officer of Special Counsel (OSC) received a whistleblower disclosure concerning employees at U.S. Customs and Border Protection's National Targeting Center-Cargo, in Herndon, Virginia alleging that employees regularly claim administratively uncontrollable overtime (AUO), but fail to perform duties that qualify for AUO. OIG assembled a taskforce to review these allegations.

The National Targeting Center did not have sufficient AUO documentation to allow us to specifically identify a violation of law, rule, or regulation. However, most of the tasks employees performed during AUO hours appear to have been administratively controllable. This report contains no recommendations.

**Evaluation of Alleged AOU Misuse by U.S. Border Patrol Agents Engaged as CrossFit Instructors****Number:** [DI-14-0539](#)**Date:** January 08, 2015

**Summary:** OIG conducted an evaluation in response to a whistleblower disclosure concerning employees in the U.S. Border Patrol (USBP) El Centro Sector Headquarters in El Centro, California alleging that agents detailed to that location as CrossFit instructors claimed administratively uncontrollable overtime (AUO) for failed to perform duties that qualify for AUO.

OIG found that AUO paid to Border Patrol agents for CrossFit instruction and related activities, such as gym maintenance and class preparation, was inconsistent with Federal AUO regulations. The hours of duty for CrossFit instruction and related activities could have been controlled administratively. In addition, CrossFit duties were not so compelling that failure to complete those duties would have constituted negligence. USBP discontinued AUO payments for CrossFit instruction and related activities in January 2014.

This report contains no recommendations.

**U.S. Customs and Border Protection's Unmanned Aircraft System Program Does Not Achieve Intended Results or Recognize All Costs of Operations****Number:** [OIG 15-17](#)**Date:** December 24, 2014

**Summary:** Although CBP's Unmanned Aircraft System program contributes to border security, after 8 years, CBP cannot prove that the program is effective because it has not developed performance measures. The program has also not achieved the expected results. Specifically, the unmanned aircraft are not meeting flight hour goals, and we found little or no evidence CBP has met its program expectations. We estimate it costs \$12,255 per flight hour to operate the program; CBP's calculation of \$2,468 per flight hour does not include all operating costs. By not recognizing all operating costs, CBP cannot accurately assess the program's cost effectiveness or make informed decisions about program expansion. In addition, Congress and the public may be unaware of all the resources committed to this program. As a result, CBP has invested significant funds in a program that has not achieved the expected results, and it cannot demonstrate how much the program has improved border security. The \$443 million CBP plans to spend on program expansion could be put to better use by investing in alternatives.

This report made four recommendations: to conduct an independent study before acquiring more unmanned aircraft, lift the limits on radar sensor operations, establish attainable goals and performance measures, and gather and report all costs of the program.

**Review of U.S. Coast Guard's FY 2014 Detailed Accounting Submission****Number:** [OIG-15-28](#)**Date:** January 23, 2015

**Summary:** Each year the OIG is required to conduct a review of all funds expended for National Drug Control Program activities during the previous fiscal year. The Office of National Drug Control Policy (ONDCP) Circular, *Accounting of Drug Control Funding and Performance*

*Summary*, requires National Drug Control Program agencies to submit a detailed accounting of all funds expended for National Drug Control Program activities to the ONDCP director no later than February 1 of each year.

KPMG LLP, under contract with OIG, issued an Independent Accountants' Report on U.S. Coast Guard's (Coast Guard) Detailed Accounting Submission. KPMG LLP's found no cause to believe the Detailed Accounting Submission for the year ended September 30, 2014 is not presented in conformity with the criteria in ONDCP's Circular. KPMG LLP did not make any recommendations as a result of its review.

### **Review of U.S. Customs and Border Protection's FY 2014 Detailed Accounting Submission**

**Number:** [OIG-15-26](#)

**Date:** January 23, 2015

**Summary:** Each year the OIG is required to conduct a review of all funds expended for National Drug Control Program activities during the previous fiscal year. The Office of National Drug Control Policy (ONDCP) Circular, *Accounting of Drug Control Funding and Performance Summary*, requires National Drug Control Program agencies to submit a detailed accounting of all funds expended for National Drug Control Program activities to the ONDCP director no later than February 1 of each year.

KPMG LLP, under contract with OIG, issued an Independent Accountants' Report on U.S. Customs and Border Protection's (CBP) fiscal year (FY) 2014 Drug Control Performance Summary Report. KPMG LLP's found no cause to believe the Performance Summary Report is not presented in conformity with the criteria in ONDCP's Circular. KPMG LLP did not make any recommendations as a result of its review.

### **The Security Posture of the United States Coast Guard's Biometrics At Sea System Needs Improvements**

**Number:** [OIG-15-41](#)

**Date:** March 3, 2015

**Summary:** The U.S. Coast Guard (USCG) operates the Biometrics at Sea System (BASS) to collect biometric data from interdicted aliens. The biometrics are sent to the Department of Homeland Security's (DHS) Biometric Identification System (IDENT) to identify potential persons of interest. The OIG audited BASS' interface with IDENT, security roles and responsibilities, and changes to control management.

OIG determined that the USCG did not have a routine reconciliation process to ensure all biometrics captured on the 23 cutters were maintained in IDENT, which may impede future identification of suspected terrorists, aggravated felons, or other persons of interest. USCG also allowed application programmers unrestricted system access to share passwords, which could result in individuals making unauthorized changes to the system without detection. Further, OIG determined that authorization for the transition from the 2-fingerprint to 10-fingerprint application system was not properly documented and the security documentation had not been updated. Without a proper authorization process USCG could not provide assurance that senior executives approved the changes prior to implementation.

OIG made seven recommendations: to reconcile with IDENT, update security documents, eliminate use of common passwords, and ensure adherence to change management policies.

### **Streamline: Measuring Its Effect on Illegal Border Crossing**

**Number:** [OIG-15-95](#)

**Date:** May 15, 2015

**Summary:** Streamline is an initiative to criminally prosecute individuals who illegally enter the United States through defined geographic regions along the Southwest border. OIG reviewed (1) whether Border Patrol measures Streamline's effectiveness; (2) whether the cost of Streamline can be determined; and (3) how Streamline affects U.S. Customs and Immigration Enforcement (ICE) Office of Removal Operations' (ERO) resources.

OIG found that although U.S. Border Patrol (CBP) Border Patrol measures streamline's effectiveness on re-entry of illegal aliens, the metrics do not reflect an alien's crossing history, re-entry, or apprehension over multiple years. Additionally, because Border Patrol does not differentiate Streamline costs from other border enforcement consequences, Border Patrol is not able to distinguish Streamline-associated costs. Finally, according to ICE ERO, Streamline has increased its workload at some of the Southwest border field offices. However, ERO cannot be certain which aliens it removes as a result of Streamline and which aliens they remove as a result of other enforcement actions.

This report also identified additional issues, such as Border Patrol not having the guidance on using Streamline for aliens who express fear of persecution on return to their home countries and inconsistencies in the use of Streamline that may violate U.S. treaty obligations.

OIG recommends measuring Streamline's effectiveness differently, estimating costs, determining appropriate staffing levels, and developing guidance on using Streamline for aliens expressing fear of persecution.

### **Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence**

**Number:** [OIG-15-137](#)

**Date:** September 02, 2015

**Summary:** U.S. Customs and Border Protection (CBP) developed the Analytical Framework for Intelligence (AFI) – an index of relevant data existing in systems – to augment the Department of Homeland Security's (DHS) gather and develop information about persons, events, and cargo of interest. OIG performed an audit to determine the status of AFI implementation and whether or not cost effective controls have been applied to protect the sensitive information processed and stored by the system.

CBP has made significant progress towards implementing AFI on schedule and within budget, and has taken measures to secure the sensitive information the system processes. In addition, CBP developed a privacy impact assessment to ensure that privacy considerations for operating AFI were addressed. Since development, system users have provided positive feedback on AFI's functionality and usefulness.

Despite these positive steps, OIG identified various deficiencies. For example, OIG identified vulnerabilities in CBP's configuration of AFI servers and applications, management of administrative accounts, contingency planning process, and plan of action and milestone process. These vulnerabilities exist because CBP did not implement all security controls according to DHS requirements. Operating AFI without effectively implementing the required security controls increases the risk of inadvertent information disclosure and service disruptions. OIG recommends CBP address these deficiencies.

### **Inspection of U.S. Customs and Border Protection Miami Field Office Ports of Entry**

**Number:** [OIG-15-13](#)

**Date:** December 18, 2014

**Summary:** U.S. Customs and Border Protection's (CBP) Office of Field Operations is responsible for port of entry operations. It enforces antiterrorism regulations, trade laws, and immigration policy at 328 ports of entry, including seaports, airports, and designated land border crossings. The Miami Field Office encompasses five ports that span 313 miles of Florida coastline, including the top two cruise ship ports in the world. In addition, there are nine airports, with Miami International ranking as the second busiest international U.S. airport and the largest cargo port for international freight. OIG conducted this review to determine if CBP Miami Field Office ports of entry comply with CBP policies and procedures.

In most instances, the CBP Miami Field Office complied with CBP policies and procedures. OIG found only minor deficiencies in CBP Miami Field Office operations for cargo targeting and seized asset management. For passenger screening, Miami International Airport leveraged an existing system to track passengers who have records for violations of laws or other significant events. Other Miami Field Office ports of entry could benefit from this "one-stop system" that would allow them to document, monitor, and report on targeting passengers in real time. The field office could improve the consistency of its recordkeeping for changes to the biometric watchlist. Also, the CBP Miami Field Office needs to improve its compliance with safeguards for using high security bolt seals during cargo screening. Lastly, the CBP Miami Field Office needs to update its policy and procedures for agriculture inspections so they align with current U.S. Department of Agriculture procedures.

## **Goal 2.2: Safeguard and Expedite Lawful Trade and Travel**

### **GAO Reports**

#### **Border Security: Progress and Challenges in DHS's Efforts to Address High-Risk Travelers and Maritime Cargo**

**Number:** [GAO-15-668T](#)

**Date:** June 02, 2015

**Summary:** In September 2013, GAO reported on actions DHS had taken to align its programs abroad with its resource use and with other U.S. governmental strategic priorities. GAO found that DHS had taken actions to better align its resource use abroad. Specifically, from 2011 to early 2012, DHS conducted a onetime review of its international footprint—the complete set of DHS

resources and efforts it has deployed abroad—and created a department-wide international engagement plan.

However, DHS had not established specific department-wide strategic priorities for resource use abroad. Specifically, DHS (1) had not established department-wide strategic priorities for international engagement, such as specific types of activities or target regions to further combating terrorism goals; (2) did not have a mechanism for monitoring alignment between resource deployment abroad and strategic priorities; and (3) did not have reliable, comparable cost data for its programs and activities abroad and had not established a standardized framework to capture these data. GAO recommended that DHS establish department-wide strategic priorities, a mechanism to routinely monitor alignment between strategic priorities and resource deployment abroad, and reliable cost data to provide DHS with critical information to make informed resource deployment decisions.

## DHS OIG Reports

### United States Coast Guard's Alteration of the Burlington Bridge Project

**Number:** [OIG-15-32](#)

**Date:** February 11, 2015

**Summary:** The U.S. Coast Guard (USCG) requested that OIG audit the accuracy of the final appropriations cost after a 2012 alteration of the BNSF Railway bridge (Burlington bridge) in Burlington Iowa.

The USCG could not provide proper documentation to support the final apportionment of cost for the Burlington bridge alteration, of which \$74 million was allocated to the USCG and \$8 million to BNSF Railway (BNSF). Specifically, the Coast Guard did not properly document its review of the construction contractors who bid on the new bridge. In addition, the financial documentation for changes to originally planned work did not always support the cost of the work. The Coast Guard also did not have a process to evaluate and verify BNSF's reported salvage value or expected savings in maintenance and repair costs. Based on our review of available documentation, OIG was unable to confirm either USCG's or BNSF's share of the final cost to alter the Burlington bridge. As a result, USCG cannot be certain it was appropriate to pay \$74 million as the Federal share of the final cost of the bridge alteration.

OIG recommended that USCG obtain supporting documentation for bridge alteration costs and review internal policies and procedures.

### U.S. Customs and Border Protection Did Not Effectively Target and Examine Rail Shipments from Canada and Mexico

**Number:** [OIG-15-39](#)

**Date:** March 03, 2015

**Summary:** OIG determined that U.S. Customs and Border Protections (CBP) did not effectively target and examine rail shipments entering the United States from Mexico and Canada. Specifically, U.S. Customs and Border Protection Officers (CBPO) did not always target systems using the mandatory Automated Targeting System (ATS). CBPOs also did not always use the

required radiation detection equipment to examine high risk shipments. Finally, CBPOs did not always record the results of their rail cargo examination in Cargo Enforcement Reporting System (CERTS).

OIG found that CBPOs were unaware of the criteria, or used inappropriate criteria. In addition, one port did not have the required equipment for its rail team, and CBPOs at two other ports used personal Radiation Detectors to examine shipments. CBPOs received insufficient training on the use of ATS and CERTS. Finally, supervisory CBPOs did not provide sufficient oversight to ensure CBPOs followed CBP policy. As a result, CBP may have failed to target or properly examine rail shipments that were at an increased risk to contain contraband or dangerous materials. In addition, CBP has no assurance that decisions to release these high-risk shipments into the U.S. were appropriate.

### **CBP's Oversight of Its Non-Intrusive Inspection Equipment Maintenance Contracts Needs Improvement**

**Number:** [OIG-15-53](#)

**Date:** March 25, 2015

**Summary:** The U.S. Customs and Border Protection's (CBP) Non-Intrusive Inspection Program (NII) is vital to securing the Nation's border while facilitating legitimate travel and trade. CBP uses NII to screen cargo and conveyances at U.S. land, sea, and air ports of entry.

In FY 2014 CBP awarded \$90.4 million in contracts and interagency agreements to perform preventative and corrective maintenance of NII equipment. OIG conducted this audit to determine if maintenance is being performed in accordance with contractual requirements and manufacturer's specifications. OIG found that CBP has not ensured that contractors performed maintenance in accordance with these requirements because they have not evaluated contractors' performance or assessed the viability of maintenance data.

OIG recommended that CBP develop a methodology and implement a plan to monitor and periodically review contractors' performance, including verification and validation of the contractor-submitted data.

### **CBP's Houston Seaport Generally Complied with Cargo Examination Requirements but Could Improve Its Documentation of Waivers and Exceptions**

**Number:** [OIG-15-64](#)

**Date:** April 14, 2015

**Summary:** OIG conducted this review to determine whether the Houston Seaport complied with U.S. Customs and Border Protection's (CBP) *National Maritime Targeting Policy* (NMTP) and *Cargo Enforcement Reporting and Tracking System* (CERTS). The Houston Seaport is the fifth largest port for arriving containers and the largest petrochemical complex in the Nation.

OIG found that the Houston Seaport generally complied with NMTP and CERTS *Port Guidance*. However, CBP could improve documentation of waivers and exceptions to mandatory examinations of high-risk cargo. In addition, CBP could improve access controls for authorizing Port Director waivers within CERTS.

**CBP is on Track to Meet ACE Milestones, but It Needs to Enhance Internal Controls****Number:** [OIG-15-91](#)**Date:** March 11, 2015

**Summary:** The Automated Commercial Environment (ACE) is the commercial trade system designed to automate border processing to enhance border security. ACE is part of a multi-year U.S. Customs and Border Protection (CBP) modernization effort that must be completed by December 2016. OIG conducted an audit to determine if CBP was track to meet its milestones for the implementation of ACE.

OIG found that CBP is on track to meet its milestones for the deployment of ACE. However, CBP has not ensured the internal control environment has kept pace with the rapid development of the ACE program. CBP has not conducted a risk assessment to identify potential gaps in data reliability and has not fully developed and implemented performance measures for the program.

OIG recommends that CBP continually assess, evaluate, and update internal controls, to include a risk assessment that identified potential data reliability gaps; and develop and implement specific, measurable, achievable, relevant, and time-sensitive performance measures.

**Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors****GAO Reports**

No GAO reports were available that aligned to this goal.

**DHS OIG Reports****Review of U.S. Immigration and Customs Enforcement's FY 2014 Detailed Accounting Submission****Number:** [OIG-15-24](#)**Date:** January 23, 2014

**Summary:** Each year the OIG is required to conduct a review of all funds expended for National Drug Control Program activities during the previous fiscal year. The Office of National Drug Control Policy (ONDCP) Circular, *Accounting of Drug Control Funding and Performance Summary*, requires National Drug Control Program agencies to submit a detailed accounting of all funds expended for National Drug Control Program activities to the ONDCP director no later than February 1 of each year.

KPMG LLP, under contract with OIG, issued an Independent Accountants' Report on Immigration and Customs Enforcement (ICE) Detailed Accounting Submission. KPMG LLP's found no cause

to believe the Detailed Accounting Submission for the year ended September 30, 2014 is not presented in conformity with the criteria in ONDCP's Circular. KPMG LLP did not make any recommendations as a result of its review.

#### **Review of U.S. Coast Guard's FY 2014 Drug Control Performance Summary Report**

**Number:** [OIG-15-27](#)

**Date:** January 26, 2015

**Summary:** Each year the OIG is required to conduct a review of all funds expended for National Drug Control Program activities during the previous fiscal year. The Office of National Drug Control Policy (ONDCP) Circular, *Accounting of Drug Control Funding and Performance Summary*, requires National Drug Control Program agencies to submit a detailed accounting of all funds expended for National Drug Control Program activities to the ONDCP director no later than February 1 of each year.

KPMG LLP, under contract with OIG, issued an Independent Accountants' Report on the U.S. Coast Guard's (USCG) FY 2014 Drug Control Performance Summary Report. KPMG LLP's found no cause to believe the Performance Summary Report for the year ended September 30, 2014 is not presented in conformity with the criteria in ONDCP's Circular. KPMG LLP did not make any recommendations as a result of its review.

#### **Review of U.S. Immigration and Customs Enforcement's FY 2014 Drug Control Performance Summary Report**

**Number:** [OIG-15-23](#)

**Date:** January 23, 2015

**Summary:** Each year the OIG is required to conduct a review of all funds expended for National Drug Control Program activities during the previous fiscal year. The Office of National Drug Control Policy (ONDCP) Circular, *Accounting of Drug Control Funding and Performance Summary*, requires National Drug Control Program agencies to submit a detailed accounting of all funds expended for National Drug Control Program activities to the ONDCP director no later than February 1 of each year.

KPMG LLP, under contract with OIG, issued an Independent Accountants' Report on Immigration and Customs Enforcement (ICE) FY 2014 Drug Control Performance Summary Report. KPMG LLP's found no cause to believe the Performance Summary Report for the year ended September 30, 2014 is not presented in conformity with the criteria in ONDCP's Circular. KPMG LLP did not make any recommendations as a result of its review.

## Mission 3: Enforce and Administer Our Immigration Laws

### Goal 3.1: Strengthen and Effectively Administer the Immigration System

#### GAO Reports

#### **H-2A and H-2B Visa Programs: Increased Protections Needed for Foreign Workers**

**Number:** [GAO-15-154](#)

**Date:** March 06, 2015

**Summary:** More than 250,000 foreign workers entered the United States through the H-2A (agricultural) and H-2B (nonagricultural) visa programs in fiscal years 2009 through 2013. U.S. employers use a process that involves multiple federal agencies to petition for and employ temporary foreign workers through these visa programs. Most workers were requested for the agriculture, horticulture, or food service industries, but DHS does not electronically maintain data on workers' occupations. DHS officials said they may capture more information on employers and job offers as the department transitions to an electronic petition system, but specifics have not been drafted.

To help prevent exploitation of and provide protections to workers, federal agencies screen employers and can impose remedies for those who violate visa program rules. However, certain limitations hinder the effectiveness of these remedies. When the Department of Labor (DOL) debars—or temporarily bans from program participation—employers who commit certain violations, it electronically captures limited information on these employers and shares it with DHS and State, which also screen employers' requests to hire workers. DOL and DHS officials said they are working on an agreement to share more information, but it has not been finalized. GAO's past work has shown that establishing guidelines on information sharing enhances interagency collaboration, which in this case could reduce the risk that some ineligible employers could be approved to hire workers. In addition, in fiscal years 2009 through 2013, DOL's H-2 employer investigations focused primarily on H-2A employers, although DOL identified some H-2B industries as high risk. DOL officials said they have not conducted a national investigations-based evaluation of H-2B employers as they have for H-2A employers. Without such an evaluation, it is unclear whether DOL's resources are being focused appropriately. Further, GAO's analysis found that about half of DOL investigations took longer than the 2-year statute of limitations on debarment. Because DOL does not collect data on the nature of the cases affected by this 2-year period, the agency cannot assess whether the statute of limitations has limited its ability to use debarment as a remedy.

GAO recommends, among other actions, that DHS publish information on jobs and recruiters; that DOL and DHS finalize their data sharing agreement; and that DOL review its H-2B enforcement efforts and collect data on cases affected by the debarment statute of limitations.

**Immigration Benefits System: Better Informed Decision Making Needed on Transformation Program****Number:** [GAO-15-415](#)**Date:** May 18, 2015

**Summary:** Each year, the U.S. Citizenship and Immigration Services' (USCIS) processes millions of applications for persons seeking to study, work, visit, or live in the United States. USCIS has been working since 2005 to transform its outdated systems into an account-based system with electronic adjudication and case management tools that will allow applicants to apply and track the progress of their application online. In 2011, USCIS reported that this effort, called the Transformation Program, was to be completed no later than June 2014 at a cost of up to \$2.1 billion. Given the critical importance of the Transformation Program, GAO was asked to review it. This report (1) discusses the program's current status, including the impact of changes made, and (2) assesses the extent to which DHS and USCIS are executing effective program oversight and governance.

USCIS currently expects its Transformation Program will cost up to \$3.1 billion and be fully deployed no later than March 2019, which is an increase of approximately \$1 billion and delay of over 4 years from its initial July 2011 baseline. In March 2012, the program began to significantly change its acquisition strategy to address various technical challenges. These changes have significantly delayed the program's planned schedule, which in turn has had adverse effects on when USCIS expects to achieve cost savings, operational efficiencies, and other benefits. Among other things, USCIS has yet to achieve the goal of enhancing national security by authenticating users and integrating with external agency databases.

While the program's two key governance bodies have taken actions aligned with leading IT management practices, neither has used reliable information to make decisions and inform external reporting. For example, one governing body's vote in March 2013 to migrate to a new architecture was based in part on savings that did not account for the added costs of merging data from the old architecture. The ability of USCIS, DHS, and Congress to effectively monitor program performance may be limited until these bodies more effectively use reliable information to inform their program evaluations.

GAO recommended that DHS components and offices improve governance and oversight of the Transformation Program.

**Immigration Benefits: Improvements Needed to Fully Implement the International Marriage Broker Regulation Act****Number:** [GAO-15-3](#)**Date:** December 10, 2014

**Summary:** Congress enacted the International Marriage Broker Regulation Act of 2005 (IMBRA) in January 2006, which aimed to address reports of domestic violence and abuse of foreign beneficiaries married or engaged to U.S. citizens who have petitioned for them to enter the United States on a K visa. As amended, IMBRA requires that the federal government collect and provide to beneficiaries information about petitioners' prior K visa petitions and criminal histories. The U.S. Citizenship and Immigration Services (USCIS) is responsible for collecting this information and adjudicating petitions, the U.S. Department of State (State) is responsible for disclosing information to beneficiaries, and the U.S. Department of Justice (DOJ) is authorized to enforce IMBRA. The

Violence Against Women Reauthorization Act of 2013 mandates that GAO report on IMBRA implementation.

This report examines the extent to which (1) DHS, State, and DOJ have implemented processes to ensure compliance with IMBRA, and (2) DHS collects and maintains reliable data to manage the K visa process.

GAO found that DHS, DOJ, and State have processes to help ensure compliance with IMBRA, as amended, but State could better document information on IMBRA disclosures. State has guidance on processes for providing IMBRA information to beneficiaries such as a pamphlet outlining for beneficiaries the K visa and legal rights and resources available to immigrant crime victims. State's guidance requires consular officers to document in State's database whether they made all of the IMBRA-required disclosures to the beneficiary during the visa interview. However, GAO's review of a sample of K visa applications showed that in about 52 percent of interview case notes (76 of 147), consular officers did not document that they had provided beneficiaries the IMBRA pamphlet as required by State's guidance. In October 2014, State drafted a guidance cable for consular officers on IMBRA implementation, including a reminder to follow guidance regarding IMBRA documentation. State's consular officer training courses, however, do not cover IMBRA-related documentation procedures outlined in its guidance. Incorporating IMBRA-related documentation requirements into training courses could help State better ensure that consular officers are aware of the requirements for documenting IMBRA disclosures.

USCIS is to collect and maintain data on, among other things, eight elements in the K visa process for GAO reporting purposes; however, six of the eight elements are either not reliable or are not collected or maintained in a reportable (i.e., electronic) format. Thus, these elements were not readily available for GAO's review. Further, USCIS officers have not consistently adjudicated I-129F petitions for K-visas or recorded complete and accurate data. Additional training for officers could help USCIS better ensure its officers are aware of IMBRA requirements to assist them in maintaining petitions data consistent with IMBRA.

GAO recommends that State provide training to consular officers on IMBRA documentation requirements. GAO also recommends, among other things, that USCIS ensure that all IMBRA-related data will be captured with the planned electronic release of the I-129F petition and that its officers receive additional training on IMBRA requirements.

## DHS OIG Reports

### USCIS' Issuance of 3-year Employment Authorization Documents Following a Federal District Court Injunction

**Number:** [OIG-15-122](#)

**Date:** August 11, 2015

**Summary:** DHS requested that OIG review the circumstances of the U.S. Citizenship and Immigration Service's (USCIS) issuance of 3-year Employment Authorization Documents (EAD) after the Federal District Court preliminary injunction of February 16, 2015.

OIG determined that a combination of factors led to the erroneous production and issuance of approximately 2,000 3-year EADs. USCIS Service Center Operations Directorate (SCOPS) management was not specific in its direction to USCIS Office of Information Technology (IT) staff. In addition, SCOPS management was mistaken in its assumption about what IT staff was able to do or had done in order to halt production of the 3-year EADs. Finally, there was a lack of understanding within IT regarding the consequences related to the release of the EADs that had been held from production.

## Goal 3.2: Prevent Unlawful Immigration

### GAO Reports

#### Central America: Information on Migration of Unaccompanied Children from El Salvador, Guatemala, and Honduras

**Number:** [GAO-15-362](#)

**Date:** February 27, 2015

**Summary:** Since 2012, there has been a rapid increase in the number of unaccompanied alien children (UAC) apprehended at the U.S.-Mexican border. According to U.S. Customs and Border Protection (CBP), the number of UAC from any country apprehended climbed from more than 24,000 in fiscal year 2012 to nearly 69,000 in fiscal year 2014. Prior to fiscal year 2012, the majority of UAC apprehended at the border were Mexican nationals. However, more than half of the UAC apprehended at the border in fiscal year 2013, and 75 percent apprehended in fiscal year 2014 were nationals of El Salvador, Guatemala, and Honduras, according to DHS/CBP. El Salvador, Guatemala, and Honduras face various socio-economic challenges, which the United States is seeking to address through assistance efforts.

GAO was asked to review issues related to U.S. assistance to Central America addressing the rapid increase in migration of UAC from El Salvador, Guatemala, and Honduras to the United States. This report identifies U.S. mission-level efforts to (1) identify causes of the rapid increase in migration of unaccompanied children and (2) address the causes identified. GAO developed a set of questions to obtain written responses from State, USAID, and DHS officials responsible for programs in El Salvador, Guatemala, and Honduras. GAO reviewed, analyzed, and tabulated these agency officials' responses.

Department of State (State), U.S. Agency for International Development (USAID), and DHS officials stationed in El Salvador, Guatemala, and Honduras most commonly identified crime and violence and economic concerns as primary causes for the recent increase in migration to the United States by UAC.

The officials reported that agencies had developed new programs and modified existing programs to address the rapid increase in UAC migration in each of the three countries. They noted that most of these programs are specifically targeted to address identified causes of migration, such as crime and violence, lack of economic opportunities, and criminal networks that smuggle unaccompanied children. For example, DHS officials reported that the department had implemented Operation Coyote, an initiative active in all three countries to combat criminal organizations involved in UAC

smuggling. According to agency officials, new and modified programs ranged in location from specific communities or cities to border areas to nation-wide or region-wide initiatives. State and USAID officials also noted that some of their efforts and strategic objectives that had been in place prior to the rapid increase in UAC migration focused on related issues such as economic development and crime reduction. Officials reported that they have undertaken various efforts to plan their responses to the increase in migration, including coordinating among U.S. agencies and with host governments. For example, agency officials from all three countries reported participating in UAC interagency working groups at each embassy. In addition, State and USAID officials said they have used DHS data on the location of origins of UAC to inform their efforts.

### **Unaccompanied Alien Children: Actions Needed to Ensure Children Receive Required Care in DHS Custody**

**Number:** [GAO-15-521](#)

**Date:** July 14, 2015

**Summary:** Between fiscal years 2009 and 2014, DHS apprehended more than 200,000 unaccompanied alien children (UAC), with the number of UAC apprehended in fiscal year 2014 being more than four times larger than that for fiscal year 2011. On the journey to the United States, many UAC have traveled thousands of miles under dangerous conditions.

The Violence Against Women Reauthorization Act of 2013 included a provision for GAO to, among other things, review how DHS cares for UAC. This report examines, among other things, the extent to which DHS has developed policies and procedures to (1) screen all UAC as required and (2) care for all UAC as required. GAO reviewed the Trafficking Victims Protection Reauthorization Act of 2008 (TVPRA) and other legal requirements, DHS policies for screening and caring for UAC, fiscal year 2009 through 2014 apprehension data on UAC, and 2014 Border Patrol UAC care data. GAO also randomly sampled and analyzed case files of Mexican UAC whom Border Patrol apprehended in fiscal year 2014. GAO interviewed DHS and HHS officials in Washington, D.C., and at Border Patrol and Office of Field Operations (OFO) facilities in Arizona, California, and Texas selected on the basis of UAC apprehension data.

Within DHS, U.S. Customs and Border Protection (CBP) has issued policies and procedures to evaluate, or screen, unaccompanied alien children (UAC)—those under 18 years old with no lawful immigration status and no parent or legal guardian in the United States available to provide care and physical custody—as required by TVPRA. However, CBP's Border Patrol agents and OFO officers who screen UAC have not consistently applied the required screening criteria or documented the rationales for decisions resulting from screening. Specifically, under TVPRA, DHS is to transfer UAC to the Department of Health and Human Services (HHS), but may allow UAC from Canada and Mexico to return to their home countries if DHS determines that UAC (1) are not victims of a severe form of trafficking in persons, (2) are not at risk of trafficking upon return, (3) do not have a fear of returning due to a credible fear of persecution, and (4) are able to make an independent decision about returning. GAO found that agents made inconsistent screening decisions, had varying levels of awareness about how they were to assess certain screening criteria, and did not consistently document the rationales for their decisions. Providing guidance on how CBP agents and officers are to assess against UAC screening criteria could better position CBP to meet legal screening requirements, and ensuring that agents document the rationales for decisions would better position CBP to review the appropriateness of these decisions.

DHS has policies in place to implement UAC care requirements, such as providing meals, and GAO's observations and interviews at 15 CBP facilities indicate that CBP generally provided care consistent with these policies at the time of GAO's visits. However, DHS does not collect complete and reliable data on care provided to UAC or the length of time UAC are in DHS custody. GAO analyzed available data on care provided to nearly 56,000 UAC apprehended by Border Patrol in fiscal year 2014 and found that agents documented 14 of 20 possible care actions for fewer than half of the UAC (the remaining 6 actions were documented for more than 50 percent of the UAC). Also, OFO has a database to record UAC care, but officers at most ports of entry do not do so. Developing and implementing processes to help ensure agents and officers record UAC care actions would provide greater assurance that DHS is meeting its care and custody requirements. Further, the interagency process to refer and transfer UAC from DHS to HHS is inefficient and vulnerable to errors because it relies on e-mails and manual data entry, and documented standard procedures, including defined roles and responsibilities, do not exist. DHS and HHS have experienced errors, such as assigning a child to two shelters at once, and holding an empty bed for 14 days at a shelter while HHS officials had placed the child elsewhere. Jointly developing a documented interagency process with defined roles and responsibilities could better position DHS and HHS to have a more efficient and effective process to refer, transfer, and place UAC in shelters.

GAO recommends that DHS, among other things, provide guidance on how agents and officers are to apply UAC screening criteria, ensure that screening decisions are documented, develop processes to record reliable data on UAC care, and document the interagency process to transfer UAC from DHS to HHS.

### **Central America: Improved Evaluation Efforts Could Enhance Agency Programs to Reduce Unaccompanied Child Migration**

**Number:** [GAO-15-707](#)

**Date:** July 29, 2015

**Summary:** According to DHS, the number of unaccompanied alien child (UAC) apprehended at the U.S.-Mexican border climbed from nearly 28,000 in fiscal year 2012 to more than 73,000 in fiscal year 2014, with nearly three-fourths of those apprehended nationals of El Salvador, Guatemala, and Honduras. Children from these three countries face a host of challenges, such as extreme violence and persistent poverty. Those who migrate can encounter even more dangers, such as robbery and abuse.

GAO was asked to review issues related to UAC migration. In February 2015, GAO reported on U.S. assistance to Central America addressing the rapid increase in UAC migration. This report reviews (1) U.S. assistance in El Salvador, Guatemala, and Honduras addressing agency-identified causes of UAC migration; (2) how agencies have determined where to locate these assistance efforts; and (3) the extent to which agencies have developed processes to assess the effectiveness of programs seeking to address UAC migration. GAO reviewed agency documents and interviewed officials in Washington, D.C., and in Central America.

U.S. agencies have sought to address causes of UAC migration through recent programs, such as information campaigns to deter migration, developed in response to the migration increase and other long-standing efforts. The recent migration increase was likely triggered, according to U.S. officials, by several emergent factors such as the increased presence and sophistication of human smugglers and confusion over U.S. immigration policy. Officials also noted that certain persistent

conditions such as violence and poverty have worsened in certain countries. In addition to long-standing efforts, such as U.S. Agency for International Development (USAID) antipoverty programs, agencies have taken new actions. For example, DHS-led investigative units have increasingly sought to disrupt human smuggling operations.

U.S. agencies have located programs based on various factors, including long-term priorities such as targeting high-poverty and -crime areas, but have adjusted to locate more programs in high-migration communities. For example, Department of State (State) officials in Guatemala said they moved programs enhancing police anticrime capabilities into such communities, and USAID officials in El Salvador said they expanded to UAC-migration-affected locations.

Most agencies have developed processes to assess the effectiveness of programs seeking to address UAC migration, but weaknesses exist in these processes for some anti-smuggling programs. For example, DHS has established performance measures, such as arrests, for units combating UAC smuggling, but has not established numeric or other types of targets for these measures, which would enable DHS to measure the units' progress. In addition, DHS and State have not always evaluated information campaigns intended to combat coyote misinformation. DHS launched its 2013 campaign in April, but launched its 2014 campaign in late June after migration levels peaked. Neither agency evaluated its 2014 campaign. Collecting performance information on media campaigns can have value in informing future campaign efforts to reduce child migration. GAO recommends that DHS and State take steps to integrate evaluations into their planning for, and implementation of, future information campaigns intended to deter migration. GAO also recommends that DHS establish performance targets for its investigative units.

## DHS OIG Reports

### U.S. Immigration and Customs Enforcement's Alternatives to Detention

**Number:** [OIG-15-22](#)

**Date:** February 04, 2015

**Summary:** U.S. Immigration and Customs Enforcement's (ICE), Intensive Supervision Appearance Program offers an alternative to detention. OIG reviewed whether: (1) the rate which program participants abscond or commit criminal acts has decreased since 2009; (2) ICE can improve the effectiveness of its alternatives to detention program by either revising the Intensive Supervision Appearance Program or through other cost-effective means; and (3) ICE's Risk Classification Assessment is Effective.

According to ICE, the Intensive Supervision Appearance Program is effective because, using according to ICE performance metrics, few program participants abscond. However, ICE has changed how it uses the program and no longer supervises some participants throughout their immigration proceedings. As a result, ICE cannot definitively determine whether the Intensive Supervision Appearance Program has reduced the rate at which aliens have absconded or been arrested for criminal acts. ICE should adjust its performance metrics to reflect changes in its criteria for program participation.

ICE instructed field offices to consider redetaining noncompliant Intensive Supervision Appearance Program participants, but most field offices do not have sufficient funding for detention bed space to accommodate all noncompliant participants. ICE could improve the effectiveness of the program by allocating some Intensive Supervision Appearance Program contract funds to redetain noncompliant participants.

ICE developed a Risk Classification Assessment to assist its release and custody classification decisions. However, the tool is time consuming, resource intensive, and not effective in determining which aliens to release or under what conditions.

### **ICE Air Transportation of Detainees Could Be More Effective**

**Number:** [OIG-15-57](#)

**Date:** April 9, 2015

**Summary:** U.S. Immigration and Customs Enforcement (ICE) Air Operations (ICE Air) is responsible for moving and removing detainees in ICE custody by providing air transportation services to Enforcement and Removal Operations' (ERO) 24 field offices.

Although ICE Air met its mission by transporting 930,435 detainees over a 3-1/2 year period, it could have used its resources more effectively. Furthermore, ICE Air does not capture the complete and accurate data essential to support operation decisions. ERO management has not developed a data management plan, assessed staffing and training needs, or implemented formal data collection policies and procedures. It also has not conducted a comprehensive analysis of current operations in order to make informed business decisions. As a result, ICE Air operated charter flights with empty seats and could have realized cost savings up to \$41.1 million upon determining optimum flight capacity.

This report recommends that ICE should develop formal policies and procedures for its air transportation program. It should ensure adequate staffing, complete and reliable program data, and perform an analysis of operations in order to identify factors affecting efficiency.

### **DHS Missing Data Needed to Strengthen its Immigration Enforcement Efforts**

**Number:** [OIG-15-85](#)

**Date:** May 04, 2015

**Summary:** DHS uses prosecutorial discretion in deciding to what extent it will enforce immigration laws, including whether to place an alien in or take them out of the removal process. However, the Department does not collect and analyze data on the use of prosecutorial discretion to fully assess its current immigration enforcement activities and to develop future policy. The Department also does not have a mechanism to continuously monitor its use of prosecutorial discretion and improve future policy.

OIG recommends that DHS Office of Policy should develop and implement a plan to collect, analyze, and report data on the use of prosecutorial discretion to assess immigration enforcement activities and policy.

## Mission 4: Safeguard and Secure Cyberspace

### Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure against Cyber Attacks and other Hazards

#### GAO Reports

##### **Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building Access Control Systems**

**Number:** 15-6

**Date:** January 12, 2015

**Summary:** The Department of Homeland Security (DHS) has taken preliminary steps to begin to understand the cyber risk to building and access controls systems in federal facilities. Some progress has been made however significant work remains. In particular DHS lacks a strategy that: (1) defines the problem, (2) identifies the roles and responsibilities, (3) analyzes the resources needed, and (4) identifies a methodology for assessing this cyber risk. The absence of a strategy that clearly defines the roles and responsibilities of key components within DHS has contributed to a lack of action within the Department. By not developing a strategy document for assessing cyber risk to facility and security systems, DHS and, in particular, NPPD have not effectively articulated a vision for organizing and prioritizing efforts to address the cyber risk facing federal facilities that DHS is responsible for protecting.

Additionally the cyber threat was not identified in the Interagency Security Committee (ISC), *Design-Basis Threat* report that identifies numerous undesirable events. An ISC official said that recent active shooter and workplace violence incidents have caused ISC to focus its efforts on policies in those areas first. Incorporating the cyber threat to building and access control systems in the *Design-Basis Threat* report will inform agencies about this threat so they can begin to assess its risk. This action also could prevent federal agencies from expending limited resources on methodologies that may result in duplication.

##### **Action Needed to Better Assess Cost-Effectiveness of Security Enhancements at Federal Facilities**

**Number:** 15-444

**Date:** March 24, 2015

**Summary:** The Interagency Security Committee (ISC) has a risk management standard that federal executive branch entities are to follow, where ISC specifies enhancements entities should implement to effectively minimize risk and meet baseline levels of protection. The ISC has identified six general categories of enhancements: interior security, facility structure, security systems, facility entrance, site improvements, and operations and administration. Enhancements can include, among other things, security systems, contract guard forces, and blast resistant windows.

The five federal entities included in this report paid for security enhancements using a range of methods such as: paying for enhancements as part of their rent to GSA; paying fees to security organizations to install or operate security screening services; and paying for enhancements during

renovation projects. Officials from the selected entities said they have used a range of practices to manage costs, such as researching and selecting the least costly vendors, considering costs in relation to risk when deciding on enhancements, and developing some performance measures. ISC's risk management standard states that federal entities should use a cost analysis methodology that considers all costs and should establish a comprehensive performance measurement and testing program to, among other things, help allocate resources. These aspects of the standard represent a rigorous approach to determining cost effectiveness and measuring performance in the security environment; however, the ISC does not provide detailed guidance or specify methodologies federal entities could use for implementation. In fact, the selected entities have had difficulty implementing these parts of the standard to the degree specified by ISC, noting that further guidance would be beneficial. ISC is well positioned to provide entities with such guidance. Implementing these parts of the standard could better able federal entities to assess the cost effectiveness of their security investments.

### **Preliminary Observations on DHS Efforts to Address Electromagnetic Threats to the Electric Grid**

**Number:** 15-692T

**Date:** July 22, 2015

**Summary:** As of July 2015, the Department of Homeland Security (DHS) reported taking several actions that could help address electromagnetic threats to the electric grid. GAO's preliminary analysis of DHS's actions indicates that they generally fell under four categories: (1) developing reports, (2) identifying mitigation efforts, (3) strategy development and planning, and (4) conducting exercises. GAO's preliminary work suggests that DHS, in conjunction with the Department of Energy (DOE), has not fully addressed a key critical infrastructure protection responsibility—identification of clear internal agency roles and responsibilities related to addressing electromagnetic threats. For example, although DHS recognized one component as the lead for assessing solar weather risks, the component has not yet identified any specific roles related to collecting or analyzing risk information.

DHS has also coordinated with federal and industry stakeholders to address some, but not all risks to the electrical grid since the EMP Commission issued its recommendations. GAO preliminarily identified eight projects in which DHS coordinated with stakeholders to help protect the grid including developing plans to address long term power outages, participation in exercises, and research and development activities. Although these are positive steps, GAO's preliminary work indicates that DHS has not effectively coordinated with stakeholders to identify critical assets or collect necessary risk information, among other responsibilities. GAO will continue to assess the issues in this statement as it completes its work and will issue a report with the final results later this year.

## DHS OIG Reports

### Oversight Review of the National Protection and Programs Directorate, Internal Affairs Division

**Number:** 15-108-IQO

**Date:** June 19, 2015

**Summary:** The OIG conducted an oversight review of the NPPD Internal Affairs Division (IAD) to focus on organizational management and investigative/inquiry management. The inquiries conducted and overseen by the IAD were found to be thorough and complete. The review did raise serious concerns about NPPD's authority to conduct criminal investigations. Additionally, the OIG found that criminal investigators assigned to IAD did not meet the minimum legal requirement of spending at least 50 percent of their time on criminal investigative activity to earn Law Enforcement Availability Pay. Lastly, the OIG found particular issues with the written policies and the overall management of inquiries.

## Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise

## GAO Reports

### Actions Needed to Address Challenges Facing Federal Systems

**Number:** 15-573T

**Date:** April 22, 2015

**Summary:** GAO has identified a number of challenges facing the government's approach to cybersecurity, including the following:

**Implementing risk-based cybersecurity programs at federal agencies:** For fiscal year 2014, 19 of 24 major federal agencies reported that deficiencies in information security controls constituted either a material weakness or significant deficiency in internal controls over their financial reporting. In addition, inspectors general at 23 of these agencies cited information security as a major management challenge for their agency.

**Securing building and access control systems:** GAO previously reported that the Department of Homeland Security lacked a strategy for addressing cyber risks to agencies' building and access control systems—computers that monitor and control building operations—and that the General Services Administration had not fully assessed the risk of cyber-attacks to such systems.

**Overseeing contractors:** The agencies GAO reviewed were inconsistent in overseeing contractors' implementation of security controls for systems they operate on behalf of agencies.

**Improving incident response:** The agencies GAO reviewed did not always effectively respond to cybersecurity incidents or develop comprehensive policies, plans, and procedures to guide incident-response activities.

**Responding to breaches of personally identifiable information:** The agencies GAO reviewed have inconsistently implemented policies and procedures for responding to data breaches involving sensitive personal information.

**Implementing security programs at small agencies:** Smaller federal agencies (generally those with 6,000 or fewer employees) have not always fully implemented comprehensive agency-wide information security programs.

Until agencies take actions to address these challenges—including the hundreds of recommendations made by GAO and inspectors general—their systems and information will be at increased risk of compromise from cyber-based attacks and other threats.

#### Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies

**Number:** 15-725T

**Date:** June 24, 2015

**Summary:** Until federal agencies take actions to address cybersecurity risks and challenges—including implementing the hundreds of recommendations GAO and agency inspectors general have made—federal systems and information, including sensitive personal information, will be at an increased risk of compromise from cyber-based attacks and other threats.

In an effort to bolster cybersecurity across the federal government, several government-wide initiatives, spearheaded by the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB), are under way. These include the following:

**Personal Identity Verification:** In 2004, the President directed the establishment of a government-wide standard for secure and reliable forms of ID for federal employees and contractor personnel who access government facilities and systems. Subsequently, OMB directed agencies to issue personal identity verification credentials to control access to federal facilities and systems. OMB recently reported that only 41 percent of user accounts at 23 civilian agencies had required these credentials for accessing agency systems.

**Continuous Diagnostics and Mitigation:** DHS, in collaboration with the General Services Administration, has established a government-wide contract for agencies to purchase tools that are intended to identify cybersecurity risks on an ongoing basis. These tools can support agencies' efforts to monitor their networks for security vulnerabilities and generate prioritized alerts to enable agency staff to mitigate the most critical weaknesses. The Department of State adopted a continuous monitoring program, and in 2011 GAO reported on the benefits of the program and challenges the department faced in implementing its approach.

**National Cybersecurity Protection System (NCPS):** This system, also referred to as EINSTEIN, is to include capabilities for monitoring network traffic and detecting and preventing intrusions, among other things. GAO has ongoing work reviewing the implementation of NCPS, and preliminary observations indicate that implementation of the intrusion detection and prevention

capabilities may be limited and DHS appears to have not fully defined requirements for future capabilities.

While these initiatives are intended to improve security, no single technology or tool is sufficient to protect against all cyber threats. Rather, agencies need to employ a multi-layered, “defense in depth” approach to security that includes well-trained personnel, effective and consistently applied processes, and appropriate technologies.

#### DHS OIG Reports

No OIG reports were available that aligned to this goal.

### Goal 4.3: Advance Cyber Law Enforcement, Incident Response, and Reporting Capabilities

#### GAO Reports

No GAO reports were available that aligned to this goal.

#### DHS OIG Reports

#### DHS Can Strengthen its Cyber Mission Coordination Efforts

**Number:** 15-140

**Date:** September 4, 2015

**Summary:** Despite some positive steps, DHS can take additional actions to strengthen its cyber mission coordination efforts. For example, the Office of Policy has not developed a cyber strategic implementation plan due to its recent establishment and limited staff. Without a strategic plan, DHS cannot effectively align the Components’ cyber responsibilities and capabilities with DHS’ overall mission. Further, DHS needs to establish a cyber training program to provide its analysts and investigators with the skills needed to effectively perform their duties at ICE, NPPD, and USSS. An automated cyber information sharing tool is needed to enhance coordination among components. Moreover, the OIG identified deficiencies regarding ICE and USSS’ implementation of DHS baseline configuration settings, vulnerability management, weakness remediation, and specialized security training that may result in loss, misuse, modification, and unauthorized access to the Department’s information systems and data.

### Goal 4.4: Strengthen the Cyber Ecosystem

#### GAO Reports

No GAO reports were available that aligned to this goal.

**DHS OIG Reports**

No OIG reports were available that aligned to this goal.

## Mission 5: Strengthen National Preparedness and Resilience

### Goal 5.1: Enhance National Preparedness

#### GAO Reports

#### **Municipalities in Fiscal Crisis: Federal Agencies Monitored Grants and Assisted Grantees, but More Could Be Done to Share Lessons Learned**

**Number:** [GAO-15-222](#)

**Date:** 3/20/2015

**Summary:** Grant management challenges experienced by municipalities in fiscal crisis. The diminished capacity of selected municipalities in fiscal crisis hindered their ability to manage federal grants in several ways. First, reductions in human capital capacity through the loss of staff greatly reduced the ability of some cities to carry out grant compliance and oversight responsibilities. Second, the loss of human capital capacity also led to grant management skills gaps. For example, in Detroit, Michigan, loss and turnover of staff with the skills to properly draw down funds caused some grant funds to remain unspent. Third, decreased financial capacity reduced some municipalities' ability to obtain federal grants. For example, both Flint, Michigan, and Stockton, California, did not apply for competitive federal grants with maintenance of effort requirements because their city governments were unable to ensure that they would maintain non-federal funding at current levels. Fourth, outdated information technology (IT) systems hampered municipalities' ability to oversee and report on federal grants. For example, Detroit's 2011 and 2012 single audits identified IT deficiencies in every federal grant program reviewed, which led to the city having to pay back some federal grant funds. In response to these challenges, the four municipalities GAO reviewed have taken a number of actions to improve their management of federal grants including centralizing their grant management processes and partnering with local nonprofits to apply for grants.

Federal grant monitoring and oversight processes. The eight grant programs GAO reviewed used, or had recently implemented, a risk-based approach to grant monitoring and oversight. These approaches applied to all grantees not just those in fiscal crisis. The grant programs administered by the Department of Housing and Urban Development (HUD) and the Department of Justice (Justice) consistently assessed grantees against a variety of risk factors to help program officials determine the need for more in-depth monitoring actions such as onsite monitoring visits. When program officials at HUD, Justice, the Department of Transportation (DOT), and the Department of Homeland Security (DHS) found deficiencies through monitoring actions, they required corrective actions from their grantees. However, in some cases, local grantees did not implement these corrective actions, resulting in continued grant management problems. In such cases, federal program officials took actions such as increasing the level of financial oversight or withholding grant funds until the grantee improved its grant management processes.

Actions taken to assist municipalities in fiscal crisis. The White House Working Group on Detroit—an interagency group assembled by the White House to assist Detroit—as well as selected agencies took a variety of actions to aid municipalities in fiscal crisis. These actions included improving collaboration between selected municipalities and federal agencies, providing

flexibilities to help grantees meet grant requirements, and offering direct technical assistance. However, neither individual agencies nor the Office of Management and Budget (OMB), which was involved in the working group and has an interagency leadership role in achieving administration policy, have formal plans to document and share lessons learned from the efforts to assist Detroit with other federal agencies and local governments.

### **Emergency Preparedness: Opportunities Exist to Strengthen Interagency Assessments and Accountability for Closing Capability Gaps**

**Number:** [GAO-15-20](#)

**Date:** 12/19/2015

**Summary:** The departments that coordinate federal emergency support functions (ESF), in preparation for national disaster response, carry out their responsibilities in various ways, but the Secretary of Homeland Security's ability to assess ESF preparedness could be enhanced. ESF coordinators conduct a range of coordination, planning, and capability assessment activities. All 10 ESF coordinators across the five departments in GAO's review reported coordinating with stakeholders and developing at least one ESF planning document. However, the ESF Leadership Group and the group's chair, the Federal Emergency Management Agency (FEMA)—a component of the Department of Homeland Security (DHS)—have not worked with other federal departments to issue supplemental guidance detailing expectations for the minimum standards for activities and product deliverables necessary to demonstrate ESF preparedness. In the absence of such guidance, GAO found that ESF coordinators are inconsistently carrying out their emergency response preparedness activities. DHS and FEMA have responsibility for assessing federal emergency preparedness. Issuing supplemental guidance detailing expectations for ESF coordinators would better enable DHS and FEMA to assess the status of ESF response preparedness.

Federal departments have identified emergency response capability gaps through national-level exercises, real-world incidents, and other assessments, but opportunities exist to help close the gaps by enhancing management oversight in two areas:

- First, federal departments are responsible for implementing their own recommended corrective actions from national-level exercises and real-world disasters, such as Hurricane Sandy, but the status of federal interagency implementation of these actions is not comprehensively collected by or reported to DHS or FEMA. As a result, DHS's and FEMA's ability to assess and report on the nation's overall preparedness is hampered.
- Second, FEMA leads interagency efforts to identify and propose actions to address capability gaps in the nation's preparedness to respond to improvised nuclear device (IND) attacks, but its implementation plan lacks key program management details. Specifically, FEMA's March 2012 IND Implementation Plan proposed over 300 recommended actions to help close gaps identified in the April 2010 DHS IND Strategy. The September 2013 annual revision to the plan contained summary information on the status of some of the recommended actions, but did not contain detailed program management information—such as specific timeframes, milestones, and estimated resources required to close any given capability gap—which is needed to better enable ongoing management oversight of gap closure efforts.

Regular reporting on the status of corrective actions identified in national-level exercises and real-world major disasters, as well as detailed program management information for management

oversight of the status of recommended actions in the IND Implementation Plan, would enhance interagency accountability for closing identified capability gaps and better enable DHS and FEMA to assess the status of federal interagency preparedness efforts.

## DHS OIG Reports

### Annual Report to Congress on States' and Urban Areas' Management of Homeland Security Grant Programs Fiscal Year 2014

**Number:** [OIG-15-14](#)

**Date:** 12/1/2014

**Summary:** This report responds to the annual reporting requirement and summarizes 18 audits completed in fiscal year 2014. The audits included about \$447 million in State Homeland Security Program and Urban Areas Security Initiative grants awarded by the Federal Emergency Management Agency (FEMA) to 13 states, 4 territories, and the District of Columbia during 3-year periods between fiscal years 2009 and 2012. During fiscal year 2014, we issued reports for Alabama, Alaska, American Samoa, Delaware, District of Columbia, Guam, Hawaii, Idaho, Iowa, Maine, New Hampshire, North Dakota, Northern Mariana Islands, Oregon, Puerto Rico, South Dakota, Vermont, and Wyoming.

In most instances, the states and urban areas administered grant programs efficiently and effectively and in compliance with grant guidance and regulations. We also identified one innovative practice that other jurisdictions could consider using.

We identified two major areas for improvement: strategic planning and oversight of grant activities. We also identified about \$14.5 million in questioned costs.

### Ohio's Management of Homeland Security Grant Program Awards for Fiscal Years 2010 Through 2012 (Revised)

**Number:** [OIG-15-67-D](#)

**Date:** 4/14/2015

**Summary:** Although Ohio took steps in recent years to improve its management of funds awarded under the HSGP, the Federal Emergency Management Agency (FEMA) cannot be assured that Ohio effectively managed grant funds from fiscal years (FY) 2010 through 2012. Specifically, Ohio needs to improve its performance measures, the accounting for grant funds, the timeliness of releasing funds to subgrantees, and its monitoring of subgrantees, including their procurement and property management practices. Although we identified many of these same challenges in two previous audits of Ohio's management of HSGP funding, FEMA has not changed its oversight practices to target Ohio's areas of repeated deficiencies. Ohio continues to disregard some Federal regulations and grant guidance. Consequently, the State may be limited in its ability to prevent, prepare for, protect against, and respond to natural disasters, acts of terrorism, and other manmade disasters.

**The Port Authority of New York and New Jersey's Recently Updated Policies, Procedures, and Business Practices Should Be Adequate to Effectively Manage FEMA Public Assistance Grant Funds****Number:** [OIG-15-67-D](#)**Date:** 4/14/2015

**Summary:** At the time of the grant award, the Port Authority of New York and New Jersey (Port Authority) did not have adequate accounting and procurement policies and procedures in place to ensure compliance with Federal Emergency Management Agency (FEMA) grant requirements. However, in late 2013, the Port Authority made changes to its accounting and procurement policies and procedures for FEMA-funded work. These changes should provide FEMA reasonable assurance that the Port Authority has the capability to account for and expend FEMA grant funds according to Federal requirements. Therefore, if the Port Authority adheres to the accounting policies and procedures it established for FEMA-funded work, it should avoid misspending the \$213 million of Public Assistance requested for Hurricane Sandy damages.

**South Carolina Department of Transportation Has Adequate Policies, Procedures, and Business Practices to Effectively Manage Its FEMA Public Assistance Grant Funding****Number:** [OIG-15-66-D](#)**Date:** 4/14/2015

**Summary:** The Department generally has established policies, procedures, and business practices to adequately account for and expend Federal Emergency Management Agency (FEMA) grant funds according to Federal regulations and FEMA guidelines. The Department has accounting systems in place to account for disaster costs on a project-by-project basis and has adequate support for costs it plans to claim under the grant award. Further, the contracts the Department awarded to accomplish work under the grant met Federal and FEMA procurement requirements.

**Audit Tips for Managing Disaster-Related Project Costs****Number:** OIG-15-100-D**Date:** [6/8/2015](#)

**Summary:** More than 100,000 recipients and subrecipients of FEMA disaster assistance grants are currently working on about 600,000 open projects worth over \$50 billion. Under the Public Assistance Program, FEMA provides grants to state, tribal, and local governments, and private nonprofit organizations so that communities can quickly respond to and recover from major disasters. FEMA's Hazard Mitigation Grant Program provides funding to the same entities to implement long-term measures to prevent damages from future disasters.

**Inspection of FEMA's Regional Offices - Region V****Number:** [OIG-15-120](#)**Date:** 8/7/2015

**Summary:** We reviewed 12 of FEMA Region V's 166 disaster-related responsibilities and determined that the region was not meeting 3 of these 12 responsibilities. Specifically, Region V did not:

- have policies and procedures to provide temporary public transportation during disasters;
- process first-level Public Assistance appeals in a timely manner; and

- hold mandated meetings to inform the Regional Administrator about the region's emergency management issues.

According to Region V officials, staffing shortages, insufficient training, and limited guidance were key factors in not meeting these responsibilities. As a result, Region V may be missing opportunities to remediate weaknesses or deficiencies in preparedness, protection, response, recovery, and mitigation activities.

### **DHS Needs to Improve Grant Guidance for Public Safety Communications Equipment**

**Number:** OIG-15-124

**Date:** [8/11/2015](#)

**Summary:** DHS provides grant guidance over the acquisition of public safety communication equipment. However, the guidance the Office of Emergency Communications and the Federal Emergency Management Agency (FEMA) issued is unclear, inconsistent, and does not prevent grantees from purchasing non-interoperable communications equipment.

The Office of Emergency Communications, within the National Protection and Programs Directorate, develops the National Emergency Communications Plan and the SAFECOM Guidance; however, neither document dictates specific requirements when purchasing emergency communications equipment. FEMA's grant guidance also does not specify interoperability requirements.

Without clear and consistent DHS grant guidance requiring interoperability, grantees could spend Federal funds for non-interoperable communications equipment purchases. Without interoperable emergency communications equipment, the lives of first responders and those of whom they are trying to assist may be at risk.

### **Summary and Key Findings of Fiscal Year 2014 FEMA Disaster Grant and Program Audits**

**Number:** [OIG-15-146-D](#)

**Date:** 9/15/2015

**Summary:** In fiscal year (FY) 2014, we issued reports on 61 audits of FEMA grants, programs, and operations funded from the Disaster Relief Fund: 49 grant audits and 12 program audits. The 61 reports contained 159 recommendations, with potential monetary benefits of \$1 billion, which included \$971.7 million reported for grant audits and \$29.3 million reported for program audits. The \$971.7 million represents 28 percent of the \$3.44 billion in grant funds we audited in FY 2014. One Hazard Mitigation Grant Program audit resulted in \$812 million of the \$971.7 million of potential monetary benefits. We continue to find problems with grant management, ineligible and unsupported costs, and noncompliance with Federal contracting requirements. The 12 program audits included 3 audits of FEMA's initial response to disasters, 4 audits related to issues we identified during our audits of FEMA's disaster responses, and 5 other audits of FEMA programs or operations. The 12 program audit reports recommended improvements to FEMA programs or operations and the recoupment of a \$29.3 million debt that a state owed to FEMA.

FEMA has been proactive in responding to our FY 2014 recommendations. As of July 15, 2015, FEMA had taken corrective actions sufficient to close 146 of the 159 recommendations, with the remaining 13 being resolved pending FEMA's completion of its planned actions. For example, FEMA Mitigation has reduced the \$812 million of unobligated funding we mention above to about

\$153 million. In addition, regarding the \$29.3 million debt, FEMA secured an agreement from the State of Louisiana to pay FEMA \$53.8 million for this debt and other overpayments.

**Table of Smaller Reports**

Date	Number	Title
6/19/2015	<a href="#">OIG-15-107</a>	New York's Management of Homeland Security Grant Program Awards for Fiscal Years 2010-12 (PDF, 94 pages - 3.43 MB)
8/7/2015	<a href="#">OIG-15-119-D</a>	Pulaski County, Missouri, Could Benefit from Additional Assistance in Managing Its FEMA Public Assistance Grant (PDF, 14 pages - 466 KB)
8/10/2015	<a href="#">OIG-15-123-D</a>	The Jackson County, Mississippi, Board of Supervisors Would Benefit from Technical Assistance in Managing Its \$14 Million FEMA Grant Award (PDF, 17 pages - 540 KB)
8/12/2015	<a href="#">OIG-15-125-D</a>	Scott County, Minnesota, Physical Development Department Has Adequate Policies, Procedures, and Business Practices to Effectively Manage Its FEMA Public Assistance Grant Funding (PDF, 10 pages - 609 KB)
8/20/2015	<a href="#">OIG-15-128-D</a>	FEMA's Process for Selecting Joint Field Offices Needs Improvement (PDF, 20 pages - 925 KB)
8/21/2015	<a href="#">OIG-15-129-D</a>	Mankato, Minnesota, Has Adequate Policies, Procedures, and Business Practices to Effectively Manage Its FEMA Public Assistance Grant Funding (PDF, 10 pages - 478 KB)
8/24/2015	<a href="#">OIG-15-132-D</a>	FEMA Should Recover \$1.78 Million of Public Assistance Grant Funds Awarded to the City of Duluth, Minnesota (PDF, 19 pages - 646 KB)
8/28/2015	<a href="#">OIG-15-135-D</a>	Napa County, California, Needs Additional Technical Assistance and Monitoring to Ensure Compliance with Federal Regulations (PDF, 16 pages - 486 KB)
8/31/2015	<a href="#">OIG-15-139-D</a>	Los Alamos County, New Mexico, Generally Accounted For and Expended FEMA Grant Funds Properly (PDF, 8 pages - 700 KB)
9/9/2015	<a href="#">OIG-15-142-D</a>	The Puerto Rico Department of Housing Did Not Properly Administer \$90.79 Million of FEMA Grant Funds Awarded for the New Secure Housing Program (PDF, 20 pages - 666 KB)
9/9/2015	<a href="#">OIG-15-143-D</a>	Rock County, Minnesota, Highway Department Has Adequate Policies, Procedures, and Business Practices to Effectively Manage Its FEMA Public Assistance Grant Funding (PDF, 10 pages - 526 KB)
9/15/2015	<a href="#">OIG-15-145-D</a>	OIG Deployment Activities at FEMA's Joint Field Office in Charleston, West Virginia -Yeager Airport (PDF, 10 pages - 543 KB)
9/19/2015	<a href="#">OIG-15-149-D</a>	FEMA Should Recover \$32.4 Million in Grant Funds Awarded to Riverside General Hospital, Houston, Texas (PDF, 27 pages - 1.09 MB)
9/30/2015	<a href="#">OIG-15-152-D</a>	Mount Carmel Baptist Church in Hattiesburg, Mississippi, Needs Assistance to Ensure Compliance with FEMA Public Assistance Grant Requirements (PDF, 17 pages - 527 KB)

## Goal 5.2: Mitigate Hazards and Vulnerabilities

### GAO Reports

No GAO reports were available that aligned to this goal.

### DHS OIG Reports

No OIG reports were available that aligned to this goal.

## Goal 5.3: Ensure Effective Emergency Response

### GAO Reports

No GAO reports were available that aligned to this goal.

### DHS OIG Reports

### FEMA Provided an Effective Response to the Napa, California, Earthquake

Number: [OIG-15-92-D](#)

Date: 5/13/2015

**Summary:** The Federal Emergency Management Agency (FEMA) responded effectively to the Napa, California, earthquake. FEMA (1) effectively coordinated activities in the heaviest affected communities before the September 11, 2014, declaration; (2) successfully executed the National Response Plan's Incident Action Planning Guide to overcome or mitigate operational challenges; and (3) effectively coordinated resources with Federal, California, and local partners while using methods to save costs in several areas. FEMA realized savings because it avoided paying for office space and other operational costs that generally total more than a million dollars for disasters similar in size as the 2014 Napa California earthquake. By February 4, 2015 FEMA had obligated \$3.4 million for the Public Assistance Grant Program and more than \$10.9 million for the Individual Assistance Program.

In addition, by deploying staff to assess FEMA's disaster response and recovery activities while they happen, we better position ourselves to identify potential problems before they occur. It also improves the quality of the recommendations we make in other reports designed to improve the disaster assistance program's integrity by preventing applicants from mispending disaster assistance funds.

**FEMA's Initial Response to the 2014 Mudslide near Oso, Washington****Number:** [OIG-15-102-D](#)**Date:** 6/10/2015

**Summary:** FEMA officials quickly and effectively responded to the disaster; were resourceful in overcoming significant challenges; implemented a variety of disaster-specific policies; obtained needed resources; and effectively coordinated with its disaster response partners. Importantly, FEMA's response effectively addressed the unique characteristics of this disaster.

In addition, by deploying staff to assess FEMA's disaster response and recovery activities while they happen, we better position ourselves to identify potential problems before they occur. It also improves the quality of the recommendations we make in other reports designed to improve the disaster assistance program's integrity by preventing applicants from misspending disaster assistance funds.

**FEMA's Initial Response to Severe Storms and Flooding in Michigan****Number:** [OIG-15-105-D](#)**Date:** 6/17/2015

**Summary:** The Federal Emergency Management Agency (FEMA) responded effectively to the 2014 Michigan storms and flooding. FEMA completed all Preliminary Damage Assessments before the declaration; overcame pressing challenges and resource shortfalls; successfully completed resource ordering; and effectively coordinated its activities with Federal, State and local partners.

In addition, by deploying to the disaster at the time of the declaration, we proactively provided FEMA and State officials with Public Assistance applicants, relevant and accurate information on our common audit findings. We particularly addressed accounting, procurement, and contracting findings.

Less than 3 weeks after the disaster declaration, FEMA had registered 69,948 disaster survivors under FEMA's Individuals and Households Program, approved \$61.6 million in individual assistance, completed 89 percent of housing inspections, opened 4 Disaster Recovery Centers, and completed 2 Kickoff meetings.

**Goal 5.4: Enable Rapid Recovery****GAO Reports****Budgeting for Disasters: Approaches to Budgeting for Disasters in Selected States****Number:** [GAO-15-424](#)**Date:** 4/27/2015

**Summary:** The 10 selected states in GAO's review—Alaska, California, Florida, Indiana, Missouri, New York, North Dakota, Oklahoma, Vermont, and West Virginia—had established budget mechanisms to ensure the availability of funding for the immediate costs of unforeseen disasters and the ongoing costs of past disasters. All 10 states provided disaster funds at the start of

the fiscal year and then as needed during the course of the fiscal year. Each of the selected states had its own combination of budget mechanisms that generally fell into four categories:

**Statewide disaster accounts.** These accounts provided the 10 states with the flexibility to fund disaster expenses across state entities or for local governments. States typically funded these accounts through general fund revenue. Six states also used other sources, such as revenues from oil and gas taxes and fees on homeowner's and commercial insurance. The amounts appropriated to these accounts at the start of the fiscal year were based on a range of considerations, such as estimates of disaster costs based on past events and emergency response costs for unforeseen disasters.

**State agency budgets.** Nine of the 10 states also covered a portion of unforeseen disaster costs through the operating or contingency budgets of state agencies with missions relevant to disaster response and recovery. For example, West Virginia's Division of Homeland Security and Emergency Management used its operating budget to cover disaster response costs. Florida's Department of Environmental Protection had a disaster contingency account funded through user fees on state parks.

**Supplemental appropriations.** When advance funding proved insufficient to cover disaster costs, eight of the 10 states provided supplemental funding to pay for the remaining costs. While reserve accounts such as rainy day funds could be used to provide this funding if general funds were unavailable, budget officials said their state rarely tapped these funds.

**Transfer authority.** All 10 states in our review allowed designated officials (i.e., the governor, budget director, or a special committee) to transfer funds within or between agencies or from statewide reserve accounts after the start of the fiscal year.

None of the 10 states in GAO's review maintained reserves dedicated solely for future disasters. Some state officials reported that they could cover disaster costs without dedicated disaster reserves because they generally relied on the federal government to fund most of the costs associated with disaster response and recovery.

While some states have increased the oversight and availability of disaster funds, all 10 states' approaches to budgeting for disasters have remained largely unchanged during fiscal years 2004 through 2013. Specifically, three states—Alaska, Indiana, and North Dakota—changed their budgeting processes to ensure that funding for disasters was appropriated before rather than after a disaster occurred. In addition, legislatures in three states—Missouri, North Dakota and West Virginia—took steps to increase their oversight of disaster spending.

### **Public Transit: Federal and Transit Agencies Taking Steps to Build Transit Systems' Resilience but Face Challenges**

**Number:** [GAO-15-159](#)

**Date:** 12/10/2015

**Summary:** The Departments of Homeland Security (DHS) and Transportation (DOT) provide funding and other support to transit agencies to help make their systems resilient to catastrophic events. DHS focuses on emergency management and security, and provides funding through its hazard-mitigation, transit-security, and other grant programs. DOT's Federal Transit Administration

(FTA) provides support through formula and discretionary-funding programs for transit capital-investment projects and for improving and maintaining existing systems. Both DHS and DOT provide transit agencies with technical assistance, such as for security programs or climate-change adaptation efforts.

Transit agencies that GAO selected identified a number of actions they are taking to help make their systems more resilient, including performing risk assessments and developing plans, such as emergency operations plans. These agencies also take actions, such as building redundant assets or facilities, to ensure the continuity of operations of the agencies' systems. Further, transit agencies have changed their infrastructure to mitigate the potential impact of disasters on their assets. For example, as shown in the figure below, one agency elevated vents and curbs to minimize water flowing into the subway.

Although all transit agencies GAO selected are taking resilience-building actions, officials GAO interviewed said that transit agencies face challenges with placing priorities on resilience and with certain aspects of some grant programs. In particular, officials from DHS, DOT, and transit agencies GAO selected explained that it is difficult for transit agencies to place priority on resilience activities because managers may be reluctant to focus on resilience and resilience activities compete with other priorities for funding. Federal, transit-agency, and emergency-management officials also cited challenges related to some aspects of federal grants that have made it difficult for transit agencies to, among other things, incorporate resilience into disaster recovery efforts and make regional transit-networks resilient. DHS, DOT, and some transit agencies are taking some actions to address these challenges, such as developing tools to help management prioritize resilience activities.

## DHS OIG Reports

### **FEMA Needs To Track Performance Data and Develop Policies, Procedures, and Performance Measures for Long Term Recovery Offices**

**Number:** [OIG-15-06-D](#)

**Date:** 10/30/2014

**Summary:** FEMA does not track costs or data associated with performance measures for Long Term Recovery Offices. Without tracking costs or data, FEMA cannot determine whether these offices are cost effective. FEMA establishes, operates, and closes Long Term Recovery Offices without standardized policies, procedures, and performance measures. Without these controls in place, FEMA is at risk for mismanagement of Federal disaster funds and cannot ensure consistency in establishing and managing these offices. Correcting these deficiencies will provide FEMA the information and guidance it needs to determine whether Long Term Recovery Offices are cost effective. In addition, FEMA can better ensure consistency in establishing and managing these offices.

### FEMA Insurance Reviews of Applicants Receiving Public Assistance Grant Funds for 2004 and 2005 Florida Hurricanes Were Not Adequate

**Number:** [OIG-15-19-D](#)

**Date:** 12/18/2014

**Summary:** The quality of FEMA’s insurance reviews in Florida was not adequate to maximize insurance available under applicants’ policies and to ensure that duplication of benefits did not occur. FEMA’s Florida Recovery Office knew about these deficiencies in its insurance review process but did not correct them. As a result, FEMA may have funded up to \$177 million that insurance should have covered.

Furthermore, FEMA’s insurance specialists routinely waived the requirement to obtain and maintain insurance for future disasters, even though they did not have the authority to take such action. FEMA’s Florida Recovery Office did not detect and correct this deficiency. As a result, FEMA potentially stands to lose up to a billion dollars in future Florida disasters because many Florida communities may not have adequate insurance coverage for future disasters such as those that occurred in 2004 and 2005.

### Table of Smaller Reports

Date	Number	Title
10/8/2014	<a href="#">OIG-15-01-D</a>	FEMA Should Recover \$13 Million of Grant Funds Awarded to The Administrators of the Tulane Educational Fund, New Orleans, Louisiana (PDF, 23 pages - 659 KB)
10/8/2014	<a href="#">OIG-15-02-D</a>	FEMA Should Recover \$3 Million of Ineligible Costs And \$4.3 Million of Unneeded Funds from the Columbus Regional Hospital (PDF, 23 pages - 2.07 MB)
10/15/2014	<a href="#">OIG-15-03-D</a>	The State of North Dakota Needs to Assist Ramsey County in Completing \$24 Million of FEMA Public Assistance Projects for Three Federally Declared Disasters that Occurred in 2009–2011 (PDF, 16 pages - 628 KB)
11/18/2014	<a href="#">OIG-15-12-D</a>	Gulfport School District, Mississippi, Properly Accounted for and Expended FEMA Public Assistance Grant Funds Awarded for Hurricane Katrina Damages (PDF, 8 pages - 486 KB)
12/9/2014	<a href="#">OIG-15-15-D</a>	Gulf Coast Mental Health Center, Mississippi, Generally Accounted for and Expended FEMA Public Assistance Grant Funds According to Federal Requirements (PDF, 10 pages - 500 MB)
1/29/2015	<a href="#">OIG-15-30-D</a>	The City of Loveland, Colorado, Could Benefit from Additional Assistance in Managing its FEMA Public Assistance Grant Funding (PDF, 17 pages - 593 KB)
2/13/2015	<a href="#">OIG-15-34-D</a>	Lamier County, Colorado, Needs Assistance to Ensure Compliance with FEMA Public Assistance Grant Requirements (PDF, 15 pages - 424 KB)
2/13/2015	<a href="#">OIG-15-35-D</a>	FEMA Should Recover \$6.2 Million of Ineligible and Unused Grant Funds Awarded to the Imperial Irrigation District, California (PDF, 13 pages - 524 KB)

Date	Number	Title
2/20/2015	<a href="#">OIG-15-37-D</a>	Gwinnett County, Georgia, Generally Accounted for and Expended FEMA Public Assistance Grant Funds According to Federal Requirements (PDF, 13 pages - 537 KB)
3/3/2015	<a href="#">OIG-15-40-D</a>	FEMA Needs to Ensure the Cost Effectiveness of \$945,640 that Los Angeles County, California Spent for Hazard Mitigation Under the Public Assistance Program (PDF, 14 pages - 673 KB)
3/18/2015	<a href="#">OIG-15-48-D</a>	FEMA Should Recover \$395,032 of Improper Contracting Costs from \$14.3 Million Grant Funds Awarded to East Jefferson General Hospital, Metairie, Louisiana (PDF, 16 pages - 591 KB)
3/18/2015	<a href="#">OIG-15-49-D</a>	Palm Beach County School District, Florida, Effectively Managed FEMA Public Assistance Grant Funds Awarded for Hurricane Frances Damages (PDF, 8 pages - 482 KB)
3/19/2015	<a href="#">OIG-15-50-D</a>	Florida and Palm Beach County School District Did Not Properly Administer \$9.2 Million of FEMA Grant Funds Awarded for Hurricane Wilma Damages (PDF, 11 pages - 422 KB)
3/19/2015	<a href="#">OIG-15-51-D</a>	Florida and the Palm Beach County School District Did Not Properly Administer \$7.7 Million of FEMA Grant Funds Awarded for Hurricane Jeanne Damages (PDF, 15 pages - 440 KB)
4/14/2015	<a href="#">OIG-15-65-D</a>	FEMA Should Disallow \$82.4 Million of Improper Contracting Costs Awarded to Holy Cross School, New Orleans, Louisiana (PDF, 26 pages - 1.44 MB)
5/7/2015	<a href="#">OIG-15-89-D</a>	FEMA Misapplied the Cost Estimating Format Resulting in an \$8 Million Overfund to the Port of Tillamook Bay, Oregon (PDF, 19 pages - 453 KB)
5/7/2015	<a href="#">OIG-15-90-D</a>	FEMA Should Recover \$2.75 Million of \$16.9 Million in Public Assistance Grant Funds Awarded to the Borough of Seaside Heights, New Jersey (PDF, 18 pages - 532 KB)
5/19/2015	<a href="#">OIG-15-96-D</a>	The City of Atlanta, Georgia, Effectively Managed FEMA Public Assistance Grant Funds Awarded for Severe Storms and Flooding in September 2009 (PDF, 8 pages - 399 KB)
6/5/2015	<a href="#">OIG-15-99-D</a>	Boulder County, Colorado, Has Adequate Policies and Procedures to Manage Its Grant, but FEMA Should Deobligate about \$2.5 Million in Unneeded Funds (PDF, 14 pages - 517 KB)
6/9/2015	<a href="#">OIG-15-101-D</a>	The Chippewa Cree Tribe of the Rocky Boy's Indian Reservation in Montana Mismanaged \$3.9 Million in FEMA Disaster Grant Funds (PDF, 17 pages - 755 KB)
6/12/2015	<a href="#">OIG-15-103-D</a>	The City of Rocky Mount, North Carolina, Effectively Managed FEMA Public Assistance Grant Funds Awarded for Hurricane Irene Damages (PDF, 8 pages - 342 KB)
6/15/2015	<a href="#">OIG-15-104-D</a>	FEMA Should Recover \$337,135 of Ineligible or Unused Grant Funds Awarded to the Port of Tillamook Bay, Oregon (PDF, 14 pages - 432 KB)

Date	Number	Title
6/17/2015	<a href="#">OIG-15-106-D</a>	Dixie Electric Membership Corporation, Greenwell Springs, Louisiana, Generally Accounted For and Expended FEMA Grants Funds Properly (PDF, 17 pages - 828 KB)
6/24/2015	<a href="#">OIG-15-109-D</a>	Kansas and the Unified School District #473 in Chapman, Kansas, Did Not Properly Administer \$50 Million of FEMA Grant Funds (PDF, 18 pages - 601 KB)
6/25/2015	<a href="#">OIG-15-110-D</a>	Lawrence County Engineer, Ohio, Generally Accounted For and Expended FEMA Grant Funds Properly (PDF, 11 pages - 504 KB)
7/1/2015	<a href="#">OIG-15-111-D</a>	FEMA Should Recover \$4.85 Million of Ineligible Grant Funds Awarded to Oklahoma City, Oklahoma (PDF, 11 pages - 533 KB)
7/16/2015	<a href="#">OIG-15-113-D</a>	FEMA Should Disallow over \$4 Million Awarded to Mountain View Electric Association, Colorado, for Improper Procurement Practices (PDF, 14 pages - 420 KB)
7/16/2015	<a href="#">OIG-15-114-D</a>	FEMA Should Recover \$9.3 Million of Ineligible and Unsupported Costs from Fox Waterway Agency in Fox Lake, Illinois (PDF, 16 pages - 484 KB)
7/21/2015	<a href="#">OIG-15-115-D</a>	Montgomery County, Maryland, Effectively Managed FEMA Public Assistance Grant Funds Awarded for Severe Storms During June and July 2012 (PDF, 9 pages - 383 KB)
7/21/2015	<a href="#">OIG-15-116-D</a>	Montgomery County, Maryland, Generally Accounted for and Expended FEMA Public Assistance Grant Funds According to Federal Requirements – Hurricane Sandy Activities (PDF, 10 pages - 417 KB)
8/20/2015	<a href="#">OIG-15-126-D</a>	The City of Napa, California, Needs Additional Technical Assistance and Monitoring to Ensure Compliance with Federal Regulations (PDF, 16pages - 712 KB)
8/20/2015	<a href="#">OIG-15-127-D</a>	Jefferson Parish, Louisiana, Generally Accounted For and Expended FEMA Grant Funds Properly (PDF, 12 pages - 383 KB)
8/21/2015	<a href="#">OIG-15-130-D</a>	The City of Kenner, Louisiana, Generally Accounted For and Expended FEMA Grant Funds Properly (PDF, 13 pages - 583 KB)
8/21/2015	<a href="#">OIG-15-131-D</a>	FEMA Should Recover \$21.7 Million of \$376 Million in Public Assistance Grant Funds Awarded to the City of Biloxi, Mississippi, for Hurricane Katrina Damages (PDF, 18 pages - 510 KB)
8/24/2015	<a href="#">OIG-15-133-D</a>	The Knoxville Utilities Board Effectively Managed FEMA Public Assistance Grant Funds Awarded for Damages from Tornadoes and Severe Storms in June 2011 (PDF, 8 pages - 483 KB)
8/24/2015	<a href="#">OIG-15-134-D</a>	The Knoxville Utilities Board Effectively Managed FEMA Public Assistance Grant Funds Awarded for Damages from Tornadoes and Severe Storms in April 2011 (PDF, 8 pages - 369 KB)

Date	Number	Title
8/28/2015	<a href="#">OIG-15-136-D</a>	FEMA Should Recover \$929,379 of Hazard Mitigation Funds Awarded to St. Tammany Parish, Louisiana (PDF, 17 pages - 479 KB)
9/9/2015	<a href="#">OIG-15-141-D</a>	FEMA Should Disallow \$2.78 Million of \$14.57 Million in Public Assistance Grant Funds Awarded to the Township of Brick, New Jersey, for Hurricane Sandy Damages (PDF, 14 pages - 533 KB)
9/15/2015	<a href="#">OIG-15-147-D</a>	Asbury Park, New Jersey, Needs Assistance in Supporting More Than \$2 Million in FEMA Grant Funds for Hurricane Sandy Debris and Emergency Work (PDF, 18 pages - 826 KB)
9/15/2015	<a href="#">OIG-15-148-D</a>	FEMA Should Recover \$4.2 Million of \$142.1 Million in Grant Funds Awarded to the City of Gulfport, Mississippi, for Hurricane Katrina Damages (PDF, 16 pages - 548 KB)
9/30/2015	<a href="#">OIG-15-151-D</a>	FEMA Should Recover \$2.0 Million in Unneeded Funds and Disallow \$1.2 Million of \$7 Million in Grant Funds Awarded to Spring Lake, New Jersey, for Hurricane Sandy (PDF, 18 pages - 1.11 MB)

## Mature and Strengthen Homeland Security

### Goal: Integrate Intelligence, Information Sharing, and Operations

#### GAO Reports

No GAO reports were available that aligned to this goal.

#### DHS OIG Reports

##### Review of DHS' Information Security Program for Intelligence Systems for Fiscal Year 2015

**Number:** 15-144

**Date:** September 11, 2015

**Summary:** The OIG reviewed the Department's security program, including its policies, procedures, and system security controls for enterprise-wide intelligence systems. Since the 2014 evaluation, the Office of Intelligence and Analysis has continued to provide effective oversight of department-wide systems and has implemented programs to monitor ongoing security practices. In addition, the Office of Intelligence and Analysis has begun relocating its intelligence system to a new location to improve network resiliency and support.

The United States Coast Guard (USCG) completed the migration of all its sites that process Top Secret/Sensitive Compartmented Information to a new system that is supported by DHS, the Defense Intelligence Agency (DIA) and USCG. USCG has coordinated with DIA to determine the ownership of this new system. However, USCG must work with DIA to fully delineate agency oversight responsibilities for the new system. In addition, deficiencies were identified in USCG's management and monitoring of the DIA-operated system.

### Goal: Enhance Partnerships and Outreach

#### GAO Reports

No GAO reports were available that aligned to this goal.

#### DHS OIG Reports

No OIG reports were available that aligned to this goal.

## Goal: Strengthen the DHS International Affairs Enterprise in Support of Homeland Security Missions

### GAO Reports

No GAO reports were available that aligned to this goal.

### DHS OIG Reports

No OIG reports were available that aligned to this goal.

## Goal: Conduct Homeland Security Research and Development

### GAO Reports

No GAO reports were available that aligned to this goal.

### DHS OIG Reports

#### Science and Technology Directorate Needs to Improve its Contract Management Procedures

**Number:** 15-38

**Date:** February 27, 2015

**Summary:** S&T properly awarded a contract to NVS Technologies, Inc. to develop technology to detect biological threats. However, S&T's lack of proper contract management procedures enabled the former Acting Director of the Chemical and Biological Defense Division to direct the termination of the contract against subject matter experts' advice. S&T terminated the contract for convenience after spending more than \$23 million for a prototype that was close to the scheduled delivery. As a result, S&T may have wasted up to \$23 million in incurred and potential contract termination costs. In addition, S&T's failure to implement policies and procedures may hinder its ability to make well-informed decisions about all of its contracts, valued at \$338 million in FY 2013. The OIG recommended that S&T develop and implement written standard operating procedures for overall contract oversight and management; develop specific procedures for terminating a contract for convenience; and review its contract portfolio to ensure sufficient evidence of program review.

## Goal: Ensure Readiness of Frontline Operators and First Responders

### GAO Reports

No GAO reports were available that aligned to this goal.

### DHS OIG Reports

#### Oversight Review of the Department of Homeland Security federal Law Enforcement Training Center Office of Professional Responsibility

**Number:** 15-04-IQO

**Date:** October 20, 2014

**Summary:** The Office of Integrity and Quality Oversight, Investigations Quality Assurance Division conducted an oversight review of the Federal Law Enforcement Training Center, Office of Professional Responsibility from June 2014 to August 2014. The review focused on two primary areas: organizational management and investigative management. In conducting the review, we assessed compliance with the DHS Management Directive 0810.1, Office of Professional Responsibility policies, and referenced guidelines established by the Council of the Inspectors General on Integrity and Efficiency, as applicable.

We found that the Office of Professional Responsibility generally complied with applicable directives, policies, guidelines, and investigative standards. We observed commendable practices with the thoroughness of investigations, the quality of reports, and the productive relationships maintained with operational entities within the Federal Law Enforcement Training Center. We found particular issues with the agency's underreporting of complaints to the Office of Inspector General, the absence of annual Law Enforcement Availability Pay documentation and certifications, and weaknesses in safeguarding evidence. We made 21 recommendations to the Office of Professional Responsibility Division Chief who agreed with them in whole or in part. There are no open recommendations in this report.

## Goal: Strengthen Service Delivery and Manage DHS Resources

### GAO Reports

#### Progress Made, but More Work Remains in Strengthening Management Functions

**Number:** 15-388T

**Date:** February 26, 2015

**Summary:** Key to addressing the department's management challenges is DHS demonstrating the ability to achieve sustained progress across 30 actions and outcomes that GAO identified and DHS agreed were needed to address the high-risk area. GAO found in its 2015 high-risk update report that DHS fully addressed 9 of these actions and outcomes, while work remains to fully address the remaining 21. Of the 9 actions and outcomes that DHS has addressed, 5 have been sustained as fully implemented for at least 2 years. For example, DHS fully met 1 outcome for the first time by

obtaining a clean opinion on its financial statements for 2 consecutive years. DHS has also mostly addressed an additional 5 actions and outcomes, meaning that a small amount of work remains to fully address them. However, DHS has partially addressed 12 and initiated 4 of the remaining actions and outcomes. For example, DHS does not have modernized financial management systems, a fact that affects its ability to have ready access to reliable information for informed decision making. Addressing some of these actions and outcomes, such as modernizing the department's financial management systems, and improving employee morale, are significant undertakings that will likely require multiyear efforts. In GAO's 2015 high-risk update report, GAO concluded that in the coming years, DHS needs to continue to show measurable, sustainable progress in implementing its key management initiatives and achieving the remaining 21 actions and outcomes.

### **DHS Should Better Define Oversight Roles and Improve Program Reporting to Congress**

**Number:** 15-292

**Date:** March 16, 2015

**Summary:** The Department of Homeland Security (DHS) has taken steps to improve oversight of major acquisition programs, but it lacks written guidance for a consistent approach to day-to-day oversight. DHS has defined the role of the Component Acquisition Executive, the senior acquisition official within each component, and established monthly meetings to discuss programs that require management attention. However, DHS has not defined all of the roles and responsibilities of the Office of Program Accountability and Risk Management (PARM)—the lead body responsible for overseeing the acquisition process and assessing the status of acquisition programs—and other headquarters organizations. GAO also found that officials' involvement and relationships with components varied significantly. DHS does not have a structure in place for overseeing the costs of 42 programs in sustainment (that is, programs that have been fielded and are operational) for which acquisition documentation requirements were waived in 2013. Sustainment costs can account for more than 80 percent of total costs, and all but one of these programs lack an approved cost estimate. GAO also previously reported that cost estimates are necessary to support decisions about program funding and resources.

The most recent data that PARM provided to DHS and congressional decision makers for oversight were not consistently accurate and up-to-date. Specifically, PARM's fiscal year 2014 Comprehensive Acquisition Status Report (CASR), which was based on fiscal year 2013 data, contained inaccurate information on DHS acquisition programs. To develop the CASR, PARM drew from DHS's official system for acquisition program reporting, the Next Generation Periodic Reporting System (nPRS); however, the system is hampered by data issues, including inconsistent participation by program officials responsible for entering the data. Further, DHS has not provided useful information for certain CASR reporting requirements. DHS interpreted one requirement in a way that eliminated the need to report cost, schedule, or performance changes for almost half of the programs in the CASR. Holding programs accountable for maintaining their data in nPRS and providing decision makers with more in-depth information would enhance future acquisition reports and render the CASR a more effective instrument for DHS and congressional oversight.

**Addressing Gaps in Oversight and Information is Key to Improving Program Outcomes****Number:** 15-541T**Date:** April 22, 2015**Summary:** GAO reported in 2012 that three key factors increase the likelihood that schedules will slip and costs will grow:

- shortfalls in program office staffing,
- gaps between needed and expected funding for programs, and
- changes to program requirements.

GAO found that these issues remain prevalent department-wide.

In March 2015, GAO reported that DHS has taken steps to improve oversight of major acquisition programs, such as defining the role of the senior acquisition official within each component and clearly defining roles and responsibilities of headquarters staff who carry out day-to-day oversight of these programs. Despite these efforts, DHS lacks key information necessary to manage its programs. For example, GAO found ambiguity across DHS testing assessments in that they did not always clearly identify whether the systems tested met all of their key performance parameters (that is, the capability or system attributes that are required to successfully meet the DHS mission). In addition, DHS's official system for acquisition program reporting—which feeds into required congressional reports—is hampered by data problems, such as inaccurate life-cycle cost estimates. As a result, the most recent data provided to DHS and congressional decision makers for oversight, through the fiscal year 2014 Comprehensive Acquisition Status Report, were not consistently accurate and up-to-date. Finally, DHS does not have information on operations and maintenance costs for 42 operational programs for which the normal documentation requirements were waived in 2013. GAO found that only one of these 42 programs has an approved life-cycle cost estimate. Operations and maintenance costs—which can account for more than 80 percent of program life-cycle costs—could run in the billions of dollars for these 42 programs.

**Major Program Assessments Reveal Actions Needed to Improve Accountability****Number:** 15-171SP**Date:** April 22, 2015**Summary:** DHS is taking steps to address enduring challenges, but certain issues may hinder oversight. DHS acquisition programs continue to face staffing, funding, and requirements issues, which increase the likelihood that acquisition programs' schedules will slip and costs will grow. DHS leadership has taken steps to address these challenges. In response to a prior GAO recommendation, DHS established that it would specifically address funding issues during all program reviews. However, it will likely take years to fully resolve the challenges. Additionally, GAO found that certain issues were prevalent at particular components. Both of the Transportation Security Administration (TSA) programs GAO reviewed have changed their scope significantly over time, but these changes are not clearly identified in their current baselines, making it difficult to assess how well the programs have been executed. In fiscal year 2014, the funding plans DHS presented to Congress for the U.S. Coast Guard (USCG) acquisition programs were incomplete, obscuring affordability issues GAO has reported on since 2011. These component-specific issues make it more challenging for DHS leadership and Congress to exercise oversight.

### Steps Taken to Enhance EAGLE II Small Business Opportunities, but Better Assessment Data Needed

**Number:** 15-551

**Date:** June 24, 2015

**Summary:** Department of Homeland Security (DHS) procurement officials reported taking three key steps to enhance small business participation in the Enterprise Acquisition Gateway for Leading-Edge Solutions II (EAGLE II) contracts:

- Creating small business tracks within each of EAGLE II's three lines of business, including socioeconomic set-aside tracks, to exclusively target competitions to small businesses in the first line of business.
- Establishing a process to maintain a steady pool of eligible small businesses by reopening the EAGLE II solicitation after requiring businesses that outgrow their small size status to leave the program.
- Requiring small business track prime contractors to team only with other small businesses.

As of March 2015, DHS had issued 74 EAGLE II task orders worth an estimated \$591 million, almost all of which—94 percent—went to small businesses. However, it is too soon to evaluate the full impact of these steps because only about 3 percent of the anticipated \$22 billion in task orders have been issued.

DHS established five goals for EAGLE II and developed performance measures to assess progress in meeting most of them. DHS established performance measures for the three EAGLE II goals related to cost savings and efficiencies through a methodology to assess cost savings, but has not fully set performance measures for the remaining two, relating to (1) the small business socioeconomic goal and (2) enhancing DHS mission capabilities. For its socioeconomic goal, DHS assesses progress via the percentage of the value of orders issued to small businesses. However, DHS does not assess whether use of team members (other small businesses) supports this goal, although DHS procurement officials told us teaming is key to enhancing small business participation. Further, DHS has not set a performance measure for assessing how the use of teaming coordinators contributes to the EAGLE II goal of enhancing DHS's mission capabilities. According to DHS, prime contractors are required to have teaming coordinators identify subcontractors with innovative services. Federal internal control standards highlight the importance of developing measures to compare expected outcomes to actual results. Without such measures, it will be difficult for DHS to have needed information to assess the extent to which the use of team members and teaming coordinators contribute toward their respective EAGLE II goals.

### Agencies Report Positive Effects of Data-Driven Reviews on Performance but Some Should Strengthen Practices

**Number:** 15-579

**Date:** July 7, 2015

**Summary:** The GPRAMA Modernization Act of 2010 (GPRAMA) requires that federal agencies review progress on agency priority goals (APG) at least once a quarter. GPRAMA requires that reviews be conducted by top agency leaders, involve APG goal leaders and other contributors, and be used to identify at-risk goals and strategies to improve performance. Since 2011, OMB has provided guidance on how reviews should be conducted, specifying they should be held in person. Further, GAO previously identified nine leading practices for reviews.

**Agencies Reported Review Practices Consistent with Requirements and Guidance.** Of the 23 agencies GAO surveyed, most reported conducting data-driven reviews consistent with requirements, guidance, and leading practices. Specifically, most agencies reported:

- conducting data-driven review meetings at least once a quarter, with several agencies holding them more frequently (20 agencies);
- conducting Chief Operating Officer (COO)-led reviews, or reviews led jointly by the COO and Performance Improvement Officer (PIO) (19);
- always or often involving PIOs (22) and APG goal leaders (21) in reviews;
- always or often collecting and analyzing relevant data in advance of reviews, and incorporating these data into meeting materials (22);
- always or often using review meetings to assess APG progress (20); and
- Always or often identifying follow-up actions to be taken after review meetings (18), an action that is positively correlated with the reported impact of reviews on agency performance improvement.

**Agency Review Practices Inconsistent with Requirements and Guidance.** Some agency practices were inconsistent with requirements or guidance. For instance, the Department of Homeland Security (DHS) reported that it does not hold in-person reviews, and the Departments of Agriculture (USDA) and Health and Human Services (HHS) reported that they do not hold regular, in-person reviews each quarter. The Department of State (State) reported that progress on each APG is only reviewed in an in-person review once a year, rather than each quarter, as required. The Department of Defense (DOD), USDA, and State also reported that their reviews are not led by their agency heads or COO. DOD also reported it rarely identifies follow-up actions to be taken after meetings.

**Agencies Reported Positive Effects of Reviews.** Most agencies reported their reviews have had positive effects on progress towards agency goals, collaboration between agency officials, the ability to hold officials accountable for progress, and efforts to improve the efficiency of operations. According to agency officials, reviews can bring together people, analytical insights, and resources to rigorously assess progress on goals or milestones, develop collaborative solutions to problems, enhance individual and collective accountability for performance, and review efforts to improve efficiency. Agencies reported that sustaining these effects requires ongoing leadership commitment, institutionalizing review processes, and demonstrating value to participants.

### **Greater Transparency Needed in Public Reporting on the Quality of Performance Information for Selected Agencies' Priority Goals**

**Number:** 15-788

**Date:** September, 10, 2015

**Summary:** The six agencies GAO reviewed generally did not publicly report on how they ensured the accuracy and reliability of performance information used to measure progress on their highest priority performance goals, referred to as agency priority goals (APGs). The GPRAMA Modernization Act of 2010 (GPRAMA) requires agencies to identify the following when publicly reporting on their APGs: 1) how performance information was verified and validated; 2) data sources; 3) level of accuracy required for intended use; 4) any limitations at the required level of accuracy; and 5) how the agency will compensate for such limitations (if needed) to reach the required level of accuracy.

GPRAMA requires agencies to provide this information to the Office of Management and Budget (OMB) for publication on Performance.gov. GPRAMA also directs agencies to provide this information for performance goals, which include APGs, in their annual performance plans and reports. While all six agencies described how they ensured the quality of their performance information overall, GAO found discussions about performance information quality addressing all five GPRAMA requirements in only the Department of Homeland Security's (DHS) performance plans and reports.

### **Agencies Need to Correct Weaknesses and Fully Implement Security Programs**

**Number:** 15-714

**Date:** September 29, 2015

**Summary:** Persistent weaknesses at 24 federal agencies illustrate the challenges they face in effectively applying information security policies and practices. Most agencies continue to have weaknesses in (1) limiting, preventing, and detecting inappropriate access to computer resources; (2) managing the configuration of software and hardware; (3) segregating duties to ensure that a single individual does not have control over all key aspects of a computer-related operation; (4) planning for continuity of operations in the event of a disaster or disruption; and (5) implementing agency-wide security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks on an ongoing basis (see fig.). These deficiencies place critical information and information systems used to support the operations, assets, and personnel of federal agencies at risk, and can impair agencies' efforts to fully implement effective information security programs. In prior reports, GAO and inspectors general have made hundreds of recommendations to agencies to address deficiencies in their information security controls and weaknesses in their programs, but many of these recommendations remain unimplemented.

Federal agencies' implementation in fiscal years 2013 and 2014 of requirements set by the *Federal Information Security Management Act of 2002* (FISMA) was mixed. For example, most agencies had developed and documented policies and procedures for managing risk, providing security training, and taking remedial actions, among other things. However, each agency's inspector general reported weaknesses in the processes used to implement FISMA requirements. In addition, to comply with FISMA's annual reporting requirements, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) provide guidance to the inspectors general on conducting and reporting agency evaluations. Nevertheless, GAO found that this guidance was not always complete, leading to inconsistent application by the inspectors general. For example, because it did not include criteria for making overall assessments, inspectors general inconsistently reported agency security performance.

### **Better Documentation Needed to Inform Future Procurements at Selected Agencies**

**Number:** 15-8

**Date:** October 9, 2014

**Summary:** Market research guidance at the Departments of Defense (DOD), Homeland Security (DHS), and Transportation (DOT) and the Federal Aviation Administration (FAA) is consistent with federal regulations in terms of market research objectives and builds on the techniques for communicating with industry outlined in federal regulations. All four agencies require that market research be clearly documented and note that documentation can inform current and future procurements. GAO found, however, that the agencies' guidance varied on the specificity of market research documentation. For example, DOD, DHS, and FAA guidance identify specific market

research elements to be documented. Based on analysis of these market research elements, GAO identified four elements which, if recorded, would provide an understanding of the research completed. These elements include the market research methods used, when it was conducted, an analysis of vendor capabilities, and a conclusion.

All 28 contracts GAO reviewed included some evidence of the market research conducted. The market research conducted on the 12 higher dollar contracts GAO reviewed tended to be more robust and include more techniques that involved outreach to vendors—such as issuing requests for information to industry—which appeared to help promote competition. Agencies did not take advantage of many available market research techniques on the 16 lower dollar contracts GAO reviewed and as a result may have missed opportunities to promote competition.

GAO also identified limitations in the market research for seven DOD and DHS lower dollar contracts that appeared to be incomplete or outdated. For example, DHS relied on incomplete information regarding potential vendors' ability to meet its requirement for parking services. Further, in 14 of the 28 contracts, the four agencies did not document one or more of four basic elements that GAO's review of agency guidance identified as important to the ability to understand the research. GAO identified this shortfall most often on lower dollar contracts reviewed at DOD and DHS. Internal control standards state that significant events need to be clearly documented so as to ensure management directives are carried out. Not documenting basic elements of the market research potentially limits the ability of agency acquisition personnel to use market research to inform future procurements, a goal identified in agency guidance.

### **DHS is Assessing Fusion Center Capabilities and Results, but Needs to More Accurately Account for Federal Funding Provided to Centers**

**Number:** 15-155

**Date:** November 6, 2014

**Summary:** The Department of Homeland Security (DHS) is helping state and major urban area fusion centers assess baseline capabilities—such as the ability to receive, analyze, and disseminate threat information—and address capability gaps through an annual assessment process, resources it provides to centers to mitigate gaps, and an exercise program to evaluate capabilities in practice. Results of the 2013 annual assessment show that centers achieved an average score of about 92 out of 100, which generally indicates that centers have policies and procedures in place to implement key information sharing activities. The scores do not reflect if these activities have resulted in specific homeland security impacts. All 10 fusion center directors GAO contacted said that the annual assessment is a useful tool to identify capabilities and monitor progress.

Since 2004, the federal government has issued guidance and related documents that define its expectations and key roles for fusion centers and also has taken steps to assess their contributions to homeland security. For example, DHS has developed 45 performance measures to help assess fusion center contributions, which generally align with attributes of successful measures. The measures include outputs—such as the number of intelligence products—and outcomes, such as how products have influenced key partners' security decisions.

In 2013, federal agencies deployed a total of 288 personnel to fusion centers. The two agencies that provide the most support—DHS's Office of Intelligence and Analysis (I&A) and the Federal Bureau of Investigation (FBI)—have developed nationwide guidance to help these agencies make fusion

center support decisions and generally identified key roles and responsibilities for personnel deployed to centers. Other DHS components, including U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, have not developed such guidance and generally defer to field-level management to make deployment decisions. However, in September 2014, DHS issued guidance that is designed to assist federal agencies in planning and tracking resource deployments to fusion centers.

DHS reforms to the Homeland Security Grant Program are helping to ensure that grant funds intended for fusion centers are used to build or sustain baseline capabilities, but DHS cannot accurately account for federal funds provided to states to support these centers. Specifically, in fiscal year 2011, the Federal Emergency Management Administration (FEMA)—the lead DHS agency responsible for grant funding—began to require that grant requests for fusion centers identify specific capabilities that proposed projects are to address. FEMA also requires that state grantees biannually report the amount of federal funds spent on fusion center projects. However, after further review of data provided to GAO, FEMA determined that states inaccurately categorized about \$60 million in projects as related to fusion centers in 2012. Thus, FEMA could not reliably report on the amount of federal grants used to support centers, which is needed to help inform future investment decisions. FEMA is developing guidance to help grantees better categorize fusion center projects and improve the reliability of grant reporting, but an additional mechanism to verify that states act in accordance with the guidance could help FEMA ensure that projects are properly classified and more accurately account for grant funding provided to centers.

### **DHS Should Take Steps to Improve Cost Reporting and Eliminate Duplicate Processing**

**Number:** 15-82

**Date:** November 19, 2014

**Summary:** The Department of Homeland Security's (DHS) *Freedom of Information Act* (FOIA) processing responsibilities are split between the department's Privacy Office, which acts as its central FOIA office, and FOIA offices in its component agencies. The Privacy Office has a number of oversight and coordination functions, including developing policies to implement FOIA initiatives, providing training, and preparing annual reports. Meanwhile, components' FOIA offices are responsible for processing the vast majority of the requests received by the department, subject to regulations and policies issued by the Privacy Office. While components report FOIA processing costs to the Privacy Office, which then aggregates and reports them to the Department of Justice, reported costs are incomplete (for example, the costs do not reflect employee benefits or the salaries of staff outside the components' FOIA offices who retrieve requested documents), thus hindering accountability for total costs. Regarding duplication, GAO determined that certain immigration-related requests are processed twice by two different DHS components. The duplicate processing of such requests by the two components contributes to an increase in the time needed to respond to the requests.

In 2011, DHS established a goal of reducing backlogged FOIA requests by 15 percent each year, and its component agencies have taken actions toward this goal, including increasing staff, reporting and monitoring backlog information, providing training, and offering incentives to staff for increased productivity. Although there was initial progress by the end of fiscal year 2012, backlog numbers do not account for an estimated 11,000 improperly closed requests, and the number of backlogged requests increased in fiscal year 2013 to a level higher than 2011.

DHS and its components have implemented or are planning to implement various technology capabilities to support FOIA processing based on best practices and federal requirements. However, not all of these systems possess all capabilities recommended by federal guidance, such as online tracking and electronic redaction, or the required capabilities to accommodate individuals with disabilities. Adopting such system capabilities department-wide could help DHS increase the efficiency of its FOIA processing.

### **Continued Action Needed to Strengthen Management of Administratively Uncontrollable Overtime**

**Number:** 15-95

**Date:** December 17, 2014

**Summary:** Department of Homeland Security (DHS) components spent \$512 million on administratively uncontrollable overtime (AUO) payments in fiscal year 2013 and \$255 million through March 2014, mostly on Border Patrol agents. DHS's AUO expenditures increased from fiscal years 2008 through 2013, in part because of higher payments per earner. The average annual AUO payment per employee increased by about 31 percent, or from about \$13,000 to about \$17,000 from fiscal years 2008 through 2013.

Some DHS component policies are not consistent with certain provisions of federal regulations or guidance, and components have not regularly followed their respective AUO policies and procedures, contributing to widespread AUO administration and oversight deficiencies. For example, components have not consistently reviewed hours claimed and employee eligibility for AUO. In response, in 2014, DHS issued two memorandums. One required the suspension of AUO for certain employees. The other required components to submit plans to address deficiencies, which most DHS components have done. DHS also plans to issue a department-wide AUO directive and to monitor component implementation of corrective actions through its ongoing human resource office assessments every 3 to 4 years, among other things. However, this monitoring is too general and infrequent to effectively monitor or evaluate DHS components' progress. Given the department's long-standing and widespread AUO administration and oversight deficiencies, developing and executing a department-wide oversight mechanism to ensure components implement AUO appropriately on a sustained basis, and in accordance with law and regulation, could better position DHS to monitor components' progress remediating AUO deficiencies. Further, DHS's reporting annually to Congress on the extent to which DHS components have made progress in remediating AUO implementation deficiencies could provide Congress with reasonable assurance that DHS components have sustained effective and appropriate use of AUO in accordance with law and regulation.

### **DHS OIG Reports**

#### **U.S. Coast Guard Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance Modernization**

**Number:** 15-05

**Date:** October 28, 2014

**Summary:** The Coast Guard has implemented information technology systems that effectively support the mission needs of some ships and aircraft. Specifically, the systems have met overall

performance requirements and have improved operational capabilities, including increased situational awareness, better communication within the Coast Guard and with its partners, and enhanced sensor capabilities. The Coast Guard, however, has not carried out some planned system enhancements that were necessary to support mission needs of certain aircraft and legacy ships. These enhancements were not carried out because of significant budget reductions. Revised plans do not fully address how the Coast Guard will meet the critical technology needs of these aircraft and legacy ships. As a result, these ships and aircraft continue to rely on obsolete technology which impacts mission performance and makes operations and maintenance more difficult and costly.

The Coast Guard has planned effectively for future technology capabilities. In particular, the Coast Guard has revised its plans to meet system needs onboard the future Offshore Patrol Cutter, which is the last major ship planned as part of fleet modernization. As a result, the new systems should support the Offshore Patrol Cutter's critical mission need, although these systems will be less capable in some areas than originally planned. The Coast Guard, however, did not have plans in place to migrate to a common system baseline for the ships and aircraft included in the modernization project, or to ensure effective support for multiple systems. As a result, the Coast Guard may experience higher life cycle costs and reduced mission effectiveness in the future.

### **Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting**

**Number:** 15-10

**Date:** November 14, 2014

**Summary:** The independent public accounting firm, KPMG LLP, has issued an unmodified (clean) opinion on the Department of Homeland Security's (DHS) consolidated financial statements. In the independent auditors' opinion, the financial statements present fairly, in all material respects, the financial position of DHS as of September 30, 2014.

KPMG LLP also issued an adverse opinion on the Department's internal control over financial reporting of s financial statements as of September 30, 2014. The report identifies seven significant deficiencies in internal control, four of which are material weaknesses. The material weaknesses are in financial reporting; information technology controls and financial systems functionality; property, plant, and equipment; and budgetary accounting. The report also identifies instances of noncompliance with four laws and regulations.

### **Major Management and Performance Challenges Facing the Department of Homeland Security (Revised)**

**Number:** 15-09

**Date:** February 23, 2015

**Summary:** We have identified major challenges that affect both the Department as a whole, as well as individual Components. DHS must continually seek to integrate management operations under an authoritative governing structure capable of effectively overseeing and managing programs that cross Component lines.

DHS must overcome the challenges inherent with uniting the Department under the Secretary's Unity of effort Initiative, as well as those over which it has little control. This year, we are reporting the Department's major challenges in the following areas:

- DHS Operations Integration
- Acquisition Management
- Financial Management
- IT Management and Privacy Issues
- Transportation Security
- Border Security and Immigration Enforcement
- Grants Management
- Employee Accountability and Integrity
- Infrastructure Protection, Cybersecurity, and Insider Threat

### Evaluation of DHS' Information Security Program for Fiscal Year 2014

**Number:** 15-16

**Date:** December 12, 2014

**Summary:** DHS has taken steps to improve its information security program. For example, DHS expanded the ongoing authorization program to improve the security of its information systems through a revised risk management approach. Additionally, DHS developed and implemented the *Fiscal Year 2014 Information Security Performance Plan*, which defines the performance requirements, priorities, and overall goals for the Department. DHS has also taken actions to address the President's cybersecurity priorities, which include the implementation of trusted internet connections, continuous monitoring of the Department's information systems, and strong authentication.

While these efforts have resulted in some improvements, Components are not consistently following DHS' policies and procedures to update the system inventory and plan of action and milestones in the Department's enterprise management systems. Further, Components continue to operate systems without the proper authority. We also identified a significant deficiency in the Department's information security program as the United States Secret Service (USSS) did not provide the Chief Information Security Officer (CISO) with the continuous monitoring data required by the Office of Management and Budget (OMB) during Fiscal Year (FY) 2014. Without this information, CISO was significantly restricted from performing continuous monitoring on the Department's information systems, managing DHS' information security program, or ensuring compliance with the President's cybersecurity priorities. Subsequent to the completion of our fieldwork, USSS established an agreement with the DHS Chief Information Officer (CIO) to provide the required data beginning in FY 2015.

### Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport (Redacted) (Revised)

**Number:** 15-18

**Date:** January 16, 2015

**Summary:** As part of our Technical Security Evaluation Program, we evaluated technical and information security policies and procedures of Department of Homeland Security components at the John F. Kennedy International Airport. Four Department components – the Transportation Security Administration, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Secret Service – operate information technology systems that support homeland security operations at this major airport.

Our evaluation focused on how these components have implemented operational, technical, and management controls for computer security at the airport and nearby locations. We performed onsite inspections of the areas where these assets were located, interviewed departmental staff, and conducted technical tests of computer security controls. We also reviewed applicable policies, procedures, and other relevant documentation.

The Department's sensitive system security policies, the information technology security controls implemented at several sites had deficiencies that, if exploited, could have resulted in the loss of confidentiality, integrity, and availability of the components' information technology systems. We identified numerous deficiencies in the information technology security controls associated with the Transportation Security Administration. Additionally, operational environmental controls and security documentation needed improvement. Further, information security vulnerabilities were not resolved timely. Technical security controls for Customs and Border Protection and Immigration and Customs Enforcement information technology resources also needed improvement. The Transportation Security Administration, Customs and Border Protection, and Immigration and Customs Enforcement did not perform required security authorization or privacy reviews on closed-circuit television and surveillance monitoring room technology. The U.S. Secret Service fully complied with DHS sensitive security policies at the airport.

### **The U.S. Coast Guard Travel to Obtain Health Care Program Needs Improved Policies and Better Oversight**

**Number:** 15-31

**Date:** February 9, 2015

**Summary:** The program did not have sufficient controls to ensure that travel for medical purposes was necessary. The Coast Guard did not establish, distribute, or ensure implementation of clear policies and procedures for reviewing, approving, and maintaining program requests. Local offices were not provided criteria or training on how to evaluate the requests, did not document that travel was necessary, and did not adequately justify that the location for medical care was appropriate.

Ninety-four percent of the records tested were missing essential information, such as physicians' referrals and cost estimates. Without this information, approving officials may not have been able to evaluate whether the travel was necessary and cost effective. As a result, the Coast Guard may have approved requests for inappropriate health care travel, incurring unnecessary costs and lost productivity.

### **The United States Secret Service Has Adequate Oversight and Management of its Acquisitions (Revised)**

**Number:** 15-21

**Date:** February 10, 2015

**Summary:** The United States Secret Service's acquisition management program office, established in 2011, has adequate oversight and management of its acquisition process, complies with DHS acquisition guidance, and has implemented some best practices. However, the Secret Service does not have its own guidance for acquisitions valued at less than \$300 million and, at the time of our audit, the component did not have a designated Component Acquisition Executive.

### **Fiscal Year 2014 Evaluation of DHS' Compliance with Federal Information Security Management Act Requirements for Intelligence Systems**

**Number:** 15-33

**Date:** February 13, 2015

**Summary:** We evaluated the Department of Homeland Security's enterprise-wide security program for Top Secret/Sensitive Compartmented Information intelligence systems. Since our fiscal year 2013 evaluation, the Office of Intelligence and Analysis (I&A) has continued to provide effective oversight of DHS' department-wide intelligence systems and established programs to monitor ongoing security Practices. For example, I&A has updated its policies and procedures, including publication of *DHS Sensitive Compartmented Information Systems Policy Directive 4300C* in September 2013. The United States Coast Guard (USCG) has relocated its headquarters to the St. Elizabeth's Campus and migrated to a new intelligence system that is now supported by the Defense Intelligence Agency, DHS, and USCG.

We identified deficiencies in I&A's configuration management and USCG's continuous monitoring, configuration management, risk management, security training, and contingency planning.

### **United States Coast Guard Has Taken Steps to Address Insider Threats, but Challenges Remain**

**Number:** 15-55

**Date:** March 27, 2015

**Summary:** USCG has taken some steps to address the risk of insider threats to its information systems and data. For example, USCG established an Insider Threat Working Group designed to implement a holistic program focused on the insider risk. In addition, USCG implemented a process to verify that system administrators have the appropriate level of access to information technology systems and networks to perform their assigned duties. Further, USCG established the Cyber Security Operations Center to monitor and respond to potential insider threat risks or incidents against USCG information systems and networks.

However, additional steps are needed to further address the risk posed by trusted insiders at USCG by:

- Implementing software to protect against the unauthorized removal of sensitive information through the use of removable media devices and email accounts;
- Implementing stronger physical security controls to protect USCG's information technology assets from possible loss, theft, destruction, or malicious actions; and
- Providing insider threat security awareness training for all USCG employees.

### **DHS Contracts and Grants Awarded through Other than Full and Open Competition, FY 2014**

**Number:** 15-59

**Date:** April 10, 2015

**Summary:** In FY 2014, DHS awarded 399 noncompetitive contracts worth about \$306 million. This represents a continuing decrease of more than \$3 billion obligated through noncompetitive contracts over a 6-year period. We reconciled the entire FY 2014 contract listing against the

Federal Procurement Data System and found that the data between the two lists were 99.8 percent identical.

Also in FY 2014, DHS awarded 66 noncompetitive grants worth about \$126 million. Although three noncompetitive grants worth approximately \$3.2 million did not meet accuracy, timeliness, or completeness standards, approximately 95.5 percent did meet the requirements as set forth in the *Federal Funding Accountability and Transparency Act of 2006*.

### **DHS Should Do More to reduce Travel Reservation Costs**

**Number:** 15-80

**Date:** April 24, 2015

**Summary:** DHS does not require components to track justifications for making travel reservations offline, that is, by contacting an agent by telephone. Therefore, it is difficult to identify whether offline travel fees are excessive. Making reservations by telephone costs \$23 to \$27 more per transaction than making a reservation online through the web-based system. The Department is also not effectively managing component's use of the online system. As a result, the Department may be missing opportunities to reduce offline travel reservation fees and identify cost savings. Finally, although the Senate Appropriations Committee expected DHS to reduce its offline reservation costs in fiscal year 2014, data from DHS showed that, overall, offline costs increased.

### **Information Technology Management Letter for the FY 2014 U.S. Customs and Border Protection Financial Statement Audit**

**Number:** 15-60

**Date:** May 6, 2015

**Summary:** We contracted with the independent public accounting firm KPMG LLP to perform the audit of the consolidated financial statements of U.S. Customs and Border Protection (CBP) and the DHS for the year ended September 30, 2014. KPMG LLP evaluated selected general information technology controls. KPMG LLP determined that CBP took corrective action by designing and consistently implementing certain account management controls.

However, KPMG LLP continued to identify deficiencies related to financial system functionality and general information technology controls regarding logical access and configuration management for CBP's core financial and feeder systems. Such control deficiencies limited CBP's ability to ensure the confidentiality, integrity, and availability of its critical financial and operational data.

### **Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport**

**Number:** 15-88

**Date:** May 7, 2015

**Summary:** We audited security controls for DHS information technology systems at San Francisco International Airport. Five Department components – U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, Management Directorate, Transportation Security Administration, and U.S. Coast Guard – operate information technology systems that support homeland security operations at this airport.

The information technology security controls implemented at these sites had deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of the components' systems. For example, physical security and environmental controls for server rooms need improvement. Additionally, DHS components were not scanning some onsite servers for vulnerabilities.

### **United States Coast Guard Safeguards for Protected Health Information Need Improvement**

**Number:** 15-87

**Date:** May 7, 2015

**Summary:** The USCG has made progress in developing a culture of privacy. Separately, the USCG Privacy Office and *Health Insurance Portability and Accountability Act (HIPAA)* Office are working to meet requirements of pertinent legislation, regulations, directives, and guidance. These offices ensure their staff annually receive mandatory privacy training, which helps embed shared attitudes, values, goals, and practices for complying with requirements to properly handle sensitive personally identifiable information and protected health information. Also, USCG has completed required privacy and security documentation for managing its information technology systems containing privacy data.

However, USCG faces challenges in protecting privacy data effectively because it lacks a strong organizational approach to resolving privacy issues. Specifically:

- USCG Privacy and HIPAA officials do not formally communicate to improve privacy oversight and incident reporting, thereby limiting USCG's ability to assess and mitigate the risks of future privacy or HIPAA breaches.
- USCG does not have consistent instructions for managing and securing the health records, potentially exposing USCG personnel and their families to loss of privacy or identity theft.
- USCG clinics have not completed contingency planning to safeguard privacy data from loss in case of disaster.
- USCG clinics lack processes to periodically review physical security, placing privacy data at unnecessary risk.
- USCG has not assessed the merchant mariner credentialing program and processes to identify and reduce risk to merchant mariners' privacy data managed throughout its geographically dispersed program operations.

### **Department of Homeland Security's FY 2014 Compliance with the Improper Payments Elimination and Recovery Act of 2010**

**Number:** 15-94

**Date:** May 13, 2015

**Summary:** During fiscal year 2014, DHS complied with the *Improper Payments Elimination and Recovery Act of 2010*. Our retesting also showed that FEMA properly performed IPERA payment testing for three programs.

Although KMPG LLP did not identify any instances of noncompliance with IPERA, DHS could improve its oversight and review of IPERA risk assessments. DHS' RM&A was delayed in approving the components' risk assessments and sample test plans, which it attributed to staffing shortages. The components began improper payment testing before obtaining RM&A's approval. In addition, neither FEMA nor RM&A noticed FEMA's omission of one program that should have

been included in its risk assessments. As a result of our review, however, FEMA did perform a risk assessment of that program.

### **Information Technology Management Letter for the FY 2014 Department of Homeland Security Financial Statement Audit**

**Number:** 15-93

**Date:** May 19, 2015

**Summary:** We contracted with the independent public accounting firm KPMG LLP (KPMG) to perform the audit of the consolidated financial statements of the DHS for FY 2014. KPMG evaluated selected general information technology (IT) controls, and IT entity-level controls, and business process application controls at DHS' components. KPMG noted that the DHS components made progress in the remediation of certain IT deficiencies we reported in FY 2013, approximately 35 percent of the prior year IT deficiencies.

KPMG continued to identify deficiencies related to access controls, segregation of duties controls, and configuration management controls of DHS' core financial system. KPMG noted that limitations in DHS components' financial systems' functionality are inhibiting the Department's ability to implement and maintain effective internal control and to effectively and efficiently process and report financial data.

The findings collectively limited DHS' ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. The deficiencies at Customs and Border Protection, the U.S. Coast Guard, and the Federal Emergency Management Agency adversely impacted the internal controls over DHS' financial reporting and its operation and collectively represent a material weakness reported in the FY 2014 DHS Agency Financial Report.

### **Corrective Actions Still Needed to Achieve Interoperable Communications**

**Number:** 15-97-VR

**Date:** May 27, 2015

**Summary:** Two and a half years ago, we published an audit, *DHS' Oversight of Interoperable Communications*, in which we tested DHS radios to determine whether DHS components could talk to each other in the event of a terrorist event or other emergency. They could not. Fewer than 0.25% of the 479 radio users we tested could access and use the specified common channel to communicate. Further, of the 382 radios tested, only 20% (78) contained all the correct program settings for the common channel.

In other words, DHS components could not talk to each other using about \$430 million worth of radios purchased. They could not do so because DHS had not established an effective governing structure with the authority and responsibility to ensure it achieved department-wide, interoperable radio communications. Although DHS had established a common radio channel to enable all components to communicate using interoperable radio systems, the channel was not mandatory.

We recently conducted a verification review to assess DHS' progress on the recommendations from our November 2012 report. Unfortunately, DHS components' inability to communicate effectively on the DHS common channel persists. Although the Department has initiated corrective actions, including a draft communications interoperability plan and draft management directives to

standardize Department-wide radio activities, these documents have not been finalized. Moreover, DHS was unable to provide a timetable for finalizing and disseminating these documents.

### **Verification Review of U.S. Coast Guard's Acquisition of the Sentinel Class – Fast Response Cutter**

**Number:** 15-78-VR

**Date:** June 1, 2015

**Summary:** The Coast Guard is acquiring the Sentinel Class Fast Response Cutter (FRC) to replace its aging Island-class patrol boats, as well as fulfill a critical need to expand its patrol boat fleet. The FRC is intended to perform multiple missions, including search and rescue, migrant interdiction, drug interdiction, and law enforcement.

In September 2008, the Coast Guard awarded an \$88.2 million fixed-price contract for the detailed design and construction of the lead FRC. The estimated \$1.5 billion contract contains 6 options to build a maximum of 34 cutters. In 2012, we reported that the Coast Guard's schedule-driven acquisition strategy allowed construction of the FRCs to start before operational, design, and technical risks were resolved. Consequently, six FRCs under construction needed modification, which increased the total cost of the acquisition by \$6.9 million and caused schedule delays of at least 270 days for each cutter. In addition, this acquisition strategy allowed the Coast Guard to procure 12 cutters before testing the new cutters in actual operational conditions. We made five recommendations to mitigate risks for the FRC, as well as future acquisitions. We determined that the Coast Guard's corrective actions met the intent of these recommendations, which we closed as of April 2013.

### **Fiscal Year 2014 Assessment of DHS Charge Card Program Indicates Moderate Risk Remains**

**Number:** 15-117

**Date:** July 31, 2015

**Summary:** DHS conducts a large volume of business using government charge cards each fiscal year. In fiscal years 2012 through 2014, DHS had more than \$400 million per year in purchase and travel card transactions.

DHS did not ensure components established documented procedures to comply with DHS requirements on charge card use. In addition, DHS components did not have sufficient oversight plans to prevent improper use of charge cards. As a result, there remains a moderate level of risk that DHS' internal controls will not prevent illegal, improper, or erroneous purchases.

### **Transportation Security Administration's Management of Its Federal Employees' Compensation Act Program**

**Number:** 15-118

**Date:** August 6, 2015

**Summary:** TSA was responsive to our 2007 report recommendations and implemented internal controls across its workers' compensation program. For example, TSA developed and implemented comprehensive policies and procedures for the submission and management of workers' compensation claims. TSA also increased the number of workers' compensation staff and implemented a strategy to address long-term, high-cost claims.

Although TSA has made progress in addressing our prior report recommendations, we noted some additional concerns. Specifically, TSA used similar but separate functions for processing workers' compensation claims without demonstrating increased effectiveness or efficiency in the processing or management of those claims. We also noted that TSA's process for reviewing the accuracy of Department of Labor's charges billed to TSA was not formally documented in its workers' compensation policy.

### **Management Advisory on department of Homeland Security Components' Reporting of Conference Spending**

**Number:** 15-121

**Date:** August 10, 2015

**Summary:** We reviewed whether, from October 1, 2013, to December 31, 2014, DHS components reported conference expenses to OIG and the public as required. During this time period, DHS components reported 28 (15 percent) of 187 conferences they were required to report to OIG; of the 28, 2 (7 percent) were reported within the required 15 days. Based on conference expenses reported in the first quarter of fiscal year 2015, the components' compliance with the reporting requirement is improving – the percentage of conferences reported rose from 13 percent in FY 2014 to 30 percent in the first quarter of FY 2015. For all but one conference with expenses exceeding \$100,000, DHS published conference expenditures on its website as required, but the public cannot easily find this information. We made three recommendations to improve DHS components' required reporting of conferences to OIG and the public. DHS concurred with these recommendations and took responsive action; we consider all three recommendations closed.

### **Accurate Reporting and Oversight Needed to Help Manage DHS' Warehouse Portfolio**

**Number:** 15-138

**Date:** August 28, 2015

**Summary:** DHS' components own and lease warehouses for a variety of reasons, such as storing disaster relief supplies, computer equipment, seized assets, and excess property. Our audit objective was to determine the effectiveness of DHS' process of assessing and managing its warehousing needs.

Although DHS has taken steps to assess its warehouses, it cannot effectively manage its warehouse needs because some of the components misclassify many of their warehouses. We found buildings that should not have been on the Department's warehouse inventory. Conversely, we found buildings that should have been classified as warehouses, but were not. Because the warehouse inventories are inaccurate, DHS cannot manage warehouses or demonstrate compliance with requirements to limit the size of real property inventories and reduce costs.

Even though most warehouses we visited were well organized and appeared to support the components' missions, we identified three warehouses that CBP could potentially consolidate or close.

### Table of Smaller Reports

Date	Number	Title
3/12/2015	<a href="#">OIG-15-42</a>	Information Technology Management Letter for the Immigration Customs Enforcement Component of the FY 2014 Department of Homeland Security Financial Statement Audit (PDF, 18 pages - 496 KB)
3/12/2015	<a href="#">OIG-15-43</a>	Information Technology Management Letter for the U.S. Citizenship and Immigration Services Component of the FY 2014 Department of Homeland Security Financial Statement Audit (PDF, 18 pages - 496 KB)
3/13/2015	<a href="#">OIG-15-44</a>	Management Letter for the FY 2014 DHS Financial Statements and Internal Control over Financial Reporting Audit (PDF, 84 pages - 1.12 MB)
3/24/2015	<a href="#">OIG-15-46</a>	Information Technology Management Letter for the Transportation Security Administration Component of the FY 2014 Department of Homeland Security Financial Statement Audit (PDF, 20 pages - 454 KB)
3/17/2015	<a href="#">OIG-15-47</a>	Information Technology Management Letter for the United States Coast Guard Component of the FY 2014 Department of Homeland Security Financial Statement Audit (PDF, 11 pages - 2.49 MB)
3/25/2015	<a href="#">OIG-15-52</a>	National Flood Insurance Program's Management Letter for DHS' FY 2014 Financial Statements Audit (Redacted) (PDF, 18 pages - 1.16 MB)
3/25/2015	<a href="#">OIG-15-54</a>	Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2014 Department of Homeland Security Financial Statement Audit (PDF, 27 pages - 619 KB)
4/8/2015	<a href="#">OIG-15-56</a>	Transportation Security Administration's Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 19 pages - 558 KB)
4/8/2015	<a href="#">OIG-15-58</a>	United States Secret Service's Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 12 pages - 481 KB)
4/14/2015	<a href="#">OIG-15-62</a>	Information Technology Management Letter for the Office of Financial Management and Office of Chief Information Officer Components of the FY 2014 Department of Homeland Security Financial Statement Audit (PDF, 17 pages - 562 KB)
4/14/2015	<a href="#">OIG-15-63</a>	Information Technology Management Letter for the Other DHS Management Components of the FY 2014 Department of Homeland Security Financial Statement Audit (PDF, 9 pages - 474 KB)
4/15/2015	<a href="#">OIG-15-68</a>	United States Coast Guards' Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 13 pages - 473 KB)

Date	Number	Title
4/15/2015	<a href="#">OIG-15-69</a>	Information Technology Management Letter for the United States Secret Service Component of the FY 2014 Department of Homeland Security Financial Statement Audit (PDF, 9 pages - 499 KB)
4/16/2015	<a href="#">OIG-15-71</a>	United States Immigration and Customs Enforcement's Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 12 pages - 436 KB)
4/17/2015	<a href="#">OIG-15-70</a>	Office of Financial Management's Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 11 pages - 457 KB)
4/21/2015	<a href="#">OIG-15-72</a>	U.S. Citizenship and Immigration Services' Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 12 pages - 492 KB)
4/21/2015	<a href="#">OIG-15-73</a>	Science and Technology Directorate's Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 10 pages - 402 KB)
4/21/2015	<a href="#">OIG-15-74</a>	National Protection and Programs Directorate's Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 11 pages - 414 KB)
4/21/2015	<a href="#">OIG-15-75</a>	Management Directorate's Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 10 pages - 1.39 MB)
4/21/2015	<a href="#">OIG-15-76</a>	Independent Auditors' Report on U.S. Customs and Border Protection's FY 2014 Financial Statements (PDF, 24 pages - 832 KB)
4/21/2015	<a href="#">OIG-15-77</a>	Federal Emergency Management Agency's Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 20 pages - 502 KB)
4/23/2015	<a href="#">OIG-15-79</a>	Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2014 Department of Homeland Security Financial Statement Audit (PDF, 16 pages - 525 KB)
4/29/2015	<a href="#">OIG-15-81</a>	Management Letter for the U.S. Customs and Border Protection's FY 2014 Consolidated Financial Statements Audit (PDF, 16 pages - 525 KB)
4/29/2015	<a href="#">OIG-15-82</a>	Office of Intelligence and Analysis and Office of Operations Coordination's Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 10 pages - 443 KB)
4/29/2015	<a href="#">OIG-15-83</a>	Federal Law Enforcement Training Centers' Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 10 pages - 472 KB)
4/29/2015	<a href="#">OIG-15-84</a>	Domestic Nuclear Detection Office's Management Letter for DHS' FY 2014 Financial Statements Audit (PDF, 9 pages - 424 KB)

## 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