



U.S. Department of Homeland Security Annual Performance Report

Fiscal Years 2014 – 2016

Appendix B: Program Evaluations



Homeland
Security

About this Report

The *U.S. Department of Homeland Security Annual Performance Report for Fiscal Years (FY) 2014 – 2016* presents the Department's performance measures and applicable results aligned to our missions, provides the planned performance targets for FY 2015 and FY 2016, and includes information on the Department's Agency Priority Goals. In addition, this report presents several FY 2014 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 2014 – 2016 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 17, 2014.
- ***DHS Annual Performance Report***: Delivery date – February 2, 2015.
- ***DHS Summary of Performance and Financial Information***: Delivery date – February 16, 2015.

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

For more information, contact:

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

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



Homeland
Security



Visit Our Website
www.dhs.gov

Table of Contents

Introduction	6
Mission 1: Prevent Terrorism and Enhance Security	7
Goal 1.1: Prevent Terrorist Attacks	7
GAO Reports	7
Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities.....	7
Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems	8
Screening Partnership Program: TSA Issued Application Guidance and Developed a Mechanism to Monitor Private versus Federal Screener Performance.....	8
Transportation Security Information Sharing: Stakeholder Satisfaction Varies; TSA Could Take Additional Actions to Strengthen Efforts.....	9
Explosives Detection Canines: TSA Has Taken Steps to Analyze Canine Team Data and Assess the Effectiveness of Passenger Screening Canines	10
Screening Partnership Program: TSA Has Improved Application Guidance and Monitoring of Screener Performance, and Continues to Improve Cost Comparison Methods	11
Secure Flight: TSA Could Take Additional Steps to Strengthen Privacy Oversight Mechanisms	12
DHS OIG Reports	13
TSA’s SPOT Program and Initial Lessons from the LAX Shooting	13
Examining TSA’s Cadre of Criminal Investigators	13
TSA’s Management of Secure 1000SP Advanced Imaging Technology Units.....	14
Vulnerabilities Exist in TSA’s Checked Baggage Screening Operations	14
Goal 1.2: Prevent and Protect Against the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities	15
GAO Reports	15
Critical Infrastructure Protection: Observations on DHS Efforts to Implement and Manage its Chemical Security Program	15
Chemical Safety: Actions Needed to Improve Federal Oversight of Facilities with Ammonium Nitrate.....	16
Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources	17
Biosurveillance: Observations on the Cancellation of BioWatch Gen-3 and Future Considerations for the Program	18
Combating Nuclear Smuggling: Past Work and Preliminary Observations on Research and Development at the Domestic Nuclear Detection Office.....	19
DHS OIG Reports	20
Domestic Nuclear Detection Office Has Taken Steps to Address Insider Threat, but Challenges Remain	20
Goal 1.3: Reduce Risk to the Nation’s Critical Infrastructure, Key Leadership, and Events	20
GAO Reports	20
Federal Protective Service: Protecting Federal Facilities Remains a Challenge	20
DHS OIG Reports	21
The Chemical Facility Anti-Terrorism Standards Authorization and Accountability Act of 2014.....	21

Mission 2: Secure and Manage Our Borders.....23

Goal 2.1: Secure U.S. Air, Land, and Sea Borders and Approaches.....23

GAO Reports.....23

Maritime Security: Progress and Challenges in Key DHS Programs to Secure the Maritime Borders.....23

Maritime Security: DHS Could Benefit from Tracking Progress in Implementing the Small Vessel Security Strategy.....24

Border Security: DHS’s Efforts to Modernize Key Enforcement Systems Could be Strengthened.....24

Arizona Border Surveillance Technology Plan: Additional Actions Needed to Strengthen Management and Assess Effectiveness.....25

Maritime Security: Progress and Challenges with Selected Port Security Programs.....26

Coast Guard: Resources Provided for Drug Interdiction Operations in the Transit Zone, Puerto Rico, and the U.S. Virgin Islands.....27

Border Security: Opportunities Exist to Strengthen Collaborative Mechanism along the Southwest Border.....28

Unmanned Aerial Systems: Department of Homeland Security’s Review of U.S. Customs and Border Protection’s Use and Compliance with Privacy and Civil Liberty Laws and Standards.....29

DHS OIG Reports.....29

Independent Review of U.S. Coast Guard’s Reporting of FY 2013 Drug Control Performance Report.....29

Review of U.S. Immigration and Customs Enforcement’s Reporting of FY 2013 Drug Control Performance Summary Report.....29

Independent Review of U.S. Customs and Border Protection’s Reporting of FY 2013 Drug Control Performance Summary Report.....30

U.S. Customs and Border Protection’s Workload Staffing Model.....30

Goal 2.2: Safeguard and Expedite Lawful Trade and Travel.....31

GAO Reports.....31

Maritime Infrastructure: Key Issues Related to Commercial Activity in the U.S. Arctic over the Next Decade.....31

Trusted Travelers: Programs Provide Benefits, but Enrollment Processes Could Be Strengthened.....32

DHS OIG Reports.....33

Enhancements in Technical Controls and Training Can Improve the Security of CBP’s Trusted Traveler Programs.....33

Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors.....34

Mission 3: Enforce and Administer Our Immigration Laws.....35

Goal 3.1: Strengthen and Effectively Administer the Immigration System.....35

GAO Reports.....35

Student and Exchange Visitor Program: DHS Needs to Assess Risks and Strengthen Oversight of Foreign Students with Employment Authorization.....35

DHS OIG Reports.....35

U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges.....35

Goal 3.2: Prevent Unlawful Immigration.....36

GAO Reports.....36

Additional Actions Could Strengthen DHS Efforts to Address Sexual Abuse	36
<i>DHS OIG Reports</i>	36
ICE’s Release of Immigration Detainees (Revised)	36
The DHS Visa Security Program	37
Mission 4: Safeguard and Secure Cyberspace	39
Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure against Cyber Attacks and other Hazards	39
<i>GAO Reports</i>	39
Federal Facilities: Selected Facilities’ Emergency Plans Generally Reflect Federal Guidance	39
GPS Disruptions: Efforts to Assess to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced	40
Critical Infrastructure: Assessment of the Department of Homeland Security’s Report on the Results of its Critical Infrastructure Partnership Streamlining Efforts	41
Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities’ Emerging Technology	41
Critical Infrastructure Protection: Observations on Key Factors in DHS’s Implementation of Its Partnership Approach.....	42
Federal Facility Security: Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards	43
Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity	44
Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts	45
Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise	46
<i>DHS OIG Reports</i>	46
Implementation Status of EINSTEIN 3 Accelerated	46
Goal 4.3: Advance Cyber Law Enforcement, Incident Response, and Reporting Capabilities	47
<i>GAO Reports</i>	47
Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent	47
Information Security: Agencies Need to Improve Cyber Incident Response Practices	48
<i>DHS OIG Reports</i>	49
DHS’ Efforts to Coordinate the Activities of Federal Cyber Operations Centers	49
Implementation Status of the Enhanced Cybersecurity Services Program	49
Goal 4.4: Strengthen the Cyber Ecosystem	50
Mission 5: Strengthen National Preparedness and Resilience	51
Goal 5.1: Enhance National Preparedness	51
<i>GAO Reports</i>	51
National Preparedness: Actions Taken by FEMA to Implement Select Provisions of the Post-Katrina Emergency Management Reform Act of 2006.....	51
Federal Emergency Management Agency: Opportunities to Achieve Efficiencies and Strengthen Operations.....	52
<i>DHS OIG Reports</i>	53

Annual Report to Congress on States’ and Urban Areas’ Management of Homeland Security Grant Programs Fiscal Year 201353

FEMA Could Realize Millions in Savings by Strengthening Policies and Internal Controls Over Grant Funding for Permanently Relocated Damaged Facilities.....53

FY 2013 FEMA Public Assistance and Hazard Mitigation Grant and Subgrant Audits54

DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures54

Goal 5.2: Mitigate Hazards and Vulnerabilities..... 55

DHS OIG Reports..... 55

 FEMA’s Dissemination of Procurement Advice Early in Disaster Response Periods55

Goal 5.3: Ensure Effective Emergency Response..... 56

GAO Reports..... 56

 Emergency Transportation Relief: Agencies Could Improve Collaboration Begun during Hurricane Sandy Response56

DHS OIG Reports..... 57

 FEMA’s Dissemination of Procurement Advice Early in Disaster Response Periods57

 FEMA Should Take Steps to Improve the Efficiency and Effectiveness of the Disaster Assistance Helpline for Disaster Survivors That Do Not Speak English or Spanish58

 FEMA’s Logistics Supply Chain Management System May Not Be Effective During a Catastrophic Disaster58

Goal 5.4: Enable Rapid Recovery 59

GAO Reports..... 59

 Hurricane Sandy Relief: Improved Guidance on Designing Internal Control Plans Could Enhance Oversight of Disaster Funding59

 National Flood Insurance Program: Progress Made on Contract Management but Monitoring and Reporting Could Be Improved.....60

 Flood Insurance: Strategies for Increasing Private Sector Involvement60

Mature and Strengthen Homeland Security 62

Goal: Integrate Intelligence, Information Sharing, and Operations..... 62

GAO Reports..... 62

 DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges.....62

DHS OIG Reports..... 63

 Lessons Learned from the Boston Marathon Bombing: Improving Intelligence and Information Sharing.....63

Goal: Enhance Partnerships and Outreach..... 63

Goal: Strengthen the DHS International Affairs Enterprise in Support of Homeland Security Missions..... 63

Goal: Conduct Homeland Security Research and Development 64

GAO Reports..... 64

 Department of Homeland Security: Continued Actions Needed to Strengthen Oversight and Coordination of Research and Development64

Goal: Ensure Readiness of Frontline Operators and First Responders 65

GAO Reports..... 65

 Improved Documentation, Resource Tracking, and Performance Measurement Could Strengthen Efforts65

Goal: Strengthen Service Delivery and Manage DHS Resources 66

GAO Reports	66
DHS Financial Management: Continued Effort Needed to Address Internal Control and System Challenges.....	66
DHS Management and Administration Spending: Reliable Data Could Help DHS Better Estimate Resource Requests.....	66
Department of Homeland Security: DHS’s Efforts to Improve Employee Morale and Fill Senior Leadership Vacancies.....	67
Strategic Sourcing: Selected Agencies Should Develop Performance Measures on Inclusion of Small Businesses and OMB Should Improve Monitoring.....	68
Homeland Security Acquisitions: DHS Could Better Manage Its Portfolio to Address Funding Gaps and Improve Communications with Congress.....	69
Information Technology: Agencies Need to Establish and Implement Incremental Development Policies.....	70
Department of Homeland Security: Progress Made; Significant Work Remains in Addressing High-Risk Areas.....	70
Coast Guard Acquisitions: Better Information on Performance and Funding Needed to Address Shortfalls.....	71
Information Security: Agencies Need to Improve Oversight of Contractor Controls.....	72
Personnel Security Clearances: Additional Guidance and Oversight Needed at DHS and DOD to Ensure Consistent Application of Revocation Process.....	73
Federal Real Property: DHS and GSA Need to Strengthen the Management of DHS Headquarters Consolidation.....	73
Inspectors General: DHS OIG's Structure, Policies, and Procedures Are Consistent with Standards, but Areas for Improvement Exist.....	74
DHS OIG Reports	76
DHS Financial Management: Investigating DHS’ Stewardship of Taxpayer Dollars.....	76
Evaluation of DHS’ Information Security Program for Fiscal Year 2013.....	76
Fiscal Year 2013 Risk Assessment of DHS Charge Card Abuse Prevention Program.....	77
The USCG’s Oversight of Recommendations from Deepwater Horizon After Action Reports.....	78
DHS’ FY 2013 Compliance with the Improper Payments Elimination and Recovery Act of 2010.....	78
Preventing Waste, Fraud, Abuse and Mismanagement in Homeland Security – a GAO High-Risk List Review.....	79
DHS Does Not Adequately Manage or Have Enforcement Authority Over its Components’ Vehicle Fleet Operations.....	80
Component Acronyms	81

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 2014 by the U.S. Government Accountability Office (GAO) and the DHS Office of Inspector General (OIG). For each report, the report name, report number, date issued, summary, and a link to the publicly released report are provided.

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

Detailed information on the findings and recommendations of FY 2014 DHS OIG reports is available at: http://www.oig.dhs.gov/index.php?option=com_content&view=article&id=210&Itemid=198.

Mission 1: Prevent Terrorism and Enhance Security

Goal 1.1: Prevent Terrorist Attacks

GAO Reports

Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities

Number: [GAO-14-159](#)

Date: November 13, 2013

Summary: Available evidence does not support whether behavioral indicators, which are used in the Transportation Security Administration's (TSA) Screening of Passengers by Observation Techniques (SPOT) program, can be used to identify persons who may pose a risk to aviation security. GAO reviewed four meta-analyses (reviews that analyze other studies and synthesize their findings) that included over 400 studies from the past 60 years and found that the human ability to accurately identify deceptive behavior based on behavioral indicators is the same as or slightly better than chance. Further, the Department of Homeland Security's (DHS) April 2011 study conducted to validate SPOT's behavioral indicators did not demonstrate their effectiveness because of study limitations, including the use of unreliable data. Twenty-one of the 25 behavior detection officers (BDO) GAO interviewed at four airports said that some behavioral indicators are subjective. TSA officials agree, and said they are working to better define them. GAO analyzed data from fiscal years 2011 and 2012 on the rates at which BDOs referred passengers for additional screening based on behavioral indicators and found that BDOs' referral rates varied significantly across airports, raising questions about the use of behavioral indicators by BDOs. To help ensure consistency, TSA officials said they deployed teams nationally to verify compliance with SPOT procedures in August 2013. However, these teams are not designed to help ensure BDOs consistently interpret SPOT indicators.

TSA has limited information to evaluate SPOT's effectiveness, but plans to collect additional performance data. The April 2011 study found that SPOT was more likely to correctly identify outcomes representing a high-risk passenger--such as possession of a fraudulent document--than through a random selection process. However, the study results are inconclusive because of limitations in the design and data collection and cannot be used to demonstrate the effectiveness of SPOT. TSA completed a performance metrics plan in November 2012 that details the performance measures required for TSA to determine whether its behavior detection activities are effective, as GAO recommended in May 2010. However, the plan notes that it will be 3 years before TSA can begin to report on the effectiveness of its behavior detection activities. Until TSA can provide scientifically validated evidence demonstrating that behavioral indicators can be used to identify passengers who may pose a threat to aviation security, the agency risks funding activities that have not been determined to be effective.

Congress should consider the absence of scientifically validated evidence for using behavioral indicators to identify threats to aviation security when assessing the potential benefits and cost in making future funding decisions for aviation security. GAO included this matter because DHS did not concur with GAO's recommendation that TSA limit future funding for these activities until it can provide such evidence, in part because DHS disagreed with GAO's analysis of indicators.

Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems**Number:** [GAO-14-357](#)**Date:** April 30, 2014

Summary: The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) does not collect or analyze available information that could be used to enhance the effectiveness of the advanced imaging technology (AIT) with automated target recognition (ATR) system. Specifically, TSA does not collect or analyze available data on drills using improvised explosive devices (IED) at the checkpoint that could provide insight into how well screening officers (SO) resolve anomalies, including objects that could pose a threat to an aircraft, identified by AIT systems, because it does not enforce compliance with its operational directive. TSA's operational directive requires personnel at airports to conduct drills to assess SO compliance with TSA's screening standard operating procedures and to train SOs to better resolve anomalies identified by AIT-ATR systems. GAO found that TSA personnel at about half of airports with AIT systems did not report any IED checkpoint drill results on those systems from March 2011 through February 2013. According to TSA, it does not ensure compliance with the directive at every airport because it is unclear which office should oversee enforcing the directive. Without data on IED checkpoint drills, TSA lacks insight into how well SOs resolve anomalies detected by AIT systems, information that could be used to help strengthen existing screening processes. Potential weaknesses in the screening process could be caused by TSA not clarifying which office is responsible for overseeing TSA's operational directive, directing that office to ensure enforcement of the directive in conducting these drills, and analyzing the data. Further, when determining AIT-ATR system effectiveness, TSA uses laboratory test results that do not reflect the combined performance of the technology, the personnel who operate it, and the process that governs AIT-related security operations. TSA officials agreed that it is important to analyze performance by including an evaluation of the technology, operators, and processes and stated that TSA is planning to assess the performance of all layers of security. By not measuring system effectiveness based on the performance of the technology and SOs who operate the technology or taking into account current processes and deployment strategies, DHS and TSA are not ensuring that future procurements meet mission needs.

TSA completed the installation of ATR software upgrades intended to address privacy concerns for all deployed AIT systems; however, it has not met proposed milestones for enhancing capabilities as documented in its AIT roadmap—a document that contains milestones for achieving enhanced capabilities to meet the agency's mission needs.

GAO recommends that TSA, among other things, clarify which office should oversee its operational directive, better measure system effectiveness, and develop a realistic schedule before procuring future generations. TSA concurred with GAO's recommendations.

Screening Partnership Program: TSA Issued Application Guidance and Developed a Mechanism to Monitor Private versus Federal Screener Performance**Number:** [GAO-14-269T](#) (Testimony)**Date:** January 14, 2014

Summary: Since GAO reported on this issue in December 2012, the Transportation Security Administration (TSA) has developed application guidance for airport operators applying to the Screening Partnership Program (SPP). In December 2012, GAO reported that TSA had not

provided guidance to airport operators on its application and approval process, which had been revised to reflect requirements in the Federal Aviation Administration Modernization and Reform Act of 2012. Further, airport operators GAO interviewed at the time generally stated that they faced difficulties completing the revised application, such as how to obtain cost information. Therefore, GAO recommended that TSA develop application guidance, and TSA concurred. To address GAO's recommendation, TSA updated its SPP website in December 2012 by providing general application guidance and a description of the criteria and process the agency uses to assess airports' SPP applications. The guidance provides examples of information that airports could consider providing to TSA to help assess their suitability for the program and also outlines how the agency will analyze cost information. The new guidance addresses the intent of GAO's recommendation and should help improve transparency of the SPP application process as well as help airport operators determine whether their airports are good candidates for the SPP.

TSA has also developed a mechanism to regularly monitor private versus federal screener performance. In December 2012, GAO found differences in performance between SPP and non-SPP airports based on its analysis of screener performance data. However, while TSA had conducted or commissioned prior reports comparing the performance of SPP and non-SPP airports, TSA officials stated at the time that they did not plan to conduct similar analyses in the future, and instead stated that they were using across-the-board mechanisms to assess screener performance across all commercial airports. In December 2012, GAO found that these across-the-board mechanisms did not summarize information for the SPP as a whole or across years, which made it difficult to identify changes in private screener performance. GAO concluded that monitoring private screener performance in comparison with federal screener performance was consistent with the statutory provision authorizing TSA to enter into contracts with private screening companies and recommended that TSA develop a mechanism to regularly monitor private versus federal screener performance. TSA concurred with the recommendation. To address GAO's recommendation, in January 2013, TSA issued its first SPP Annual Report, which provides an analysis of private versus federal screener performance. Further, in September 2013, a TSA Assistant Administrator signed an operations directive that provides internal guidance for preparing the SPP Annual Report, including the requirement that the report annually verify that the level of screening services and protection provided at SPP airports is equal to or greater than the level that would be provided by federal screeners. These actions address the intent of GAO's recommendation and could assist TSA in identifying performance changes that could lead to improvements in the program.

Transportation Security Information Sharing: Stakeholder Satisfaction Varies; TSA Could Take Additional Actions to Strengthen Efforts

Number: [GAO-14-506](#)

Date: June 24, 2014

Summary: Satisfaction with the Transportation Security Administration's (TSA) security-related products and the mechanisms used to disseminate them varied by transportation mode, and TSA has not used the results of GAO's 2011 survey of stakeholders to identify the causes of information-sharing gaps or actions to address them. Assessing the results of GAO's current survey could better position TSA to look for causes of such gaps and identify solutions to improve its information-sharing efforts.

TSA has some mechanisms in place to collect stakeholder feedback, such as surveys attached to its products and informal feedback collected at meetings with stakeholders, but TSA has not systematically obtained, documented, and incorporated stakeholder feedback to improve information sharing. TSA is beginning to take steps to systematically obtain stakeholder satisfaction survey data. However, TSA is in the initial planning stages of this effort and has not determined whether or how it plans to document informal feedback—used by the majority of stakeholders GAO surveyed—or identified how it plans to incorporate all of the feedback collected. Consistent with customer service best practices, TSA could better ensure it is meeting stakeholder needs by including in its planned framework a systematic process to document informal feedback, and how it plans to incorporate all of the feedback it receives, both formal and informal.

Among other things, GAO recommends that TSA assess GAO's survey results to identify causes of information-sharing gaps and actions to address them, and systematically document and incorporate stakeholder feedback. DHS concurred.

Explosives Detection Canines: TSA Has Taken Steps to Analyze Canine Team Data and Assess the Effectiveness of Passenger Screening Canines

Number: [GAO-14-695T](#) (Testimony)

Date: June 24, 2014

Summary: In January 2013, GAO reported that the Transportation Security Administration (TSA) collected and used key canine program data in support of its National Explosives Detection Canine Team Program (NEDCTP), but could better analyze these data to identify program trends. For example, GAO found that in reviewing short notice assessments (covert tests), TSA did not analyze the results beyond the pass and fail rates. Therefore, TSA was missing an opportunity to determine if there were any search areas or types of explosives in which canine teams were more effective compared with others, and what, if any, training may be needed to mitigate deficiencies. GAO recommended that TSA regularly analyze available data to identify program trends and areas that are working well and those in need of corrective action to guide program resources and activities. TSA concurred and has taken actions that address the intent of our recommendation. For example, in the event a team fails a short notice assessment, TSA now requires that canine team supervisors complete an analysis of the team's training records to identify an explanation for the failure.

In January 2013, GAO found that TSA began deploying passenger screening canine (PSC) teams—teams of canines trained to detect explosives being carried or worn on a person—in April 2011 prior to determining the teams' operational effectiveness and where within an airport PSC teams would be most effectively utilized. GAO recommended that TSA expand and complete testing to assess the effectiveness of PSCs and conventional canines (trained to detect explosives in stationary objects) in all airport areas deemed appropriate prior to making additional PSC deployments. This would help (1) determine whether PSCs are effective at screening passengers, and resource expenditures for PSC training are warranted, and (2) inform decisions regarding the type of canine team to deploy and where to optimally deploy such teams. TSA concurred and has taken steps to address the recommendation, but additional action is needed. Specifically, TSA launched a PSC training and assessment initiative and determined PSCs to be most effective when working at the airport checkpoint, but TSA does not plan to conduct a comparison of PSC teams with conventional canine teams as GAO recommended. In January 2013, GAO also found that TSA's 2012 Strategic Framework calls for the deployment of PSC teams based on risk; however, airport stakeholder concerns related to the composition and capabilities of PSC teams resulted in the teams not being

deployed to the highest-risk airports. GAO recommended that if PSCs are determined to provide an enhanced security benefit compared with conventional canine teams, TSA should coordinate with airport stakeholders to deploy future PSC teams to the highest-risk airports. TSA concurred and has taken steps to address the recommendation. Specifically, the PSC teams for which TSA had funding and not already deployed to a specific airport at the time GAO's report was issued have been deployed to, or allocated to, the highest-risk airports.

Screening Partnership Program: TSA Has Improved Application Guidance and Monitoring of Screener Performance, and Continues to Improve Cost Comparison Methods

Number: [GAO-14-787T](#) (Testimony)

Date: July 29, 2014

Summary: Since GAO's December 2012 report on the Screening Partnership Program (SPP), the Transportation Security Administration (TSA) has developed guidance for airport operators applying to the SPP. In December 2012, GAO found that TSA had not provided guidance to airport operators on its SPP application and approval process, which had been revised to reflect statutory requirements. Further, airport operators GAO interviewed at the time identified difficulties in completing the revised application, such as obtaining cost information requested in the application. GAO recommended that TSA develop application guidance and TSA concurred. In December 2012, TSA updated its SPP website with general application guidance and a description of TSA's assessment criteria and process. The new guidance addresses the intent of GAO's recommendation.

TSA has also developed a mechanism to regularly monitor private versus federal screener performance. In December 2012, TSA officials stated that they planned to assess overall screener performance across all commercial airports instead of comparing the performance of SPP and non-SPP airports as they had done previously. Also in December 2012, GAO reported differences between the performance at SPP and non-SPP airports based on screener performance data. In addition, GAO reported that TSA's across-the-board mechanisms did not summarize information for the SPP as a whole or across years, making it difficult to identify changes in private screener performance. GAO concluded that monitoring and comparing private and federal screener performance were consistent with the statutory provision authorizing TSA to contract with private screening companies. As a result, GAO recommended that TSA develop a mechanism to regularly do so. TSA concurred with the recommendation and in January 2013, issued its *SPP Annual Report*, which provided an analysis of private versus federal screener performance. In September 2013, TSA provided internal guidance requiring that the report annually verify that the level of screening services and protection provided at SPP airports is equal to or greater than the level that would be provided by federal screeners. These actions address the intent of GAO's recommendation.

TSA has faced challenges in accurately comparing the costs of screening services at SPP and non-SPP airports. In 2007, TSA estimated that SPP airports cost about 17 percent more to operate than airports using federal screeners. In January 2009, GAO noted strengths in TSA's methodology, but also identified seven limitations that could affect the accuracy and reliability of cost comparisons. GAO recommended that TSA update its analysis to address the limitations. TSA generally concurred with the recommendation. In March 2011, TSA described efforts to address the limitations and a revised cost comparison estimating that SPP airports would cost 3 percent more to operate in 2011 than airports using federal screeners. In March 2011, GAO found that TSA had taken steps to address some of the limitations, but needed to take additional actions. In July 2014,

TSA officials stated that they are continuing to make additional changes to the cost estimation methodology and GAO is continuing to monitor TSA's progress in this area through ongoing work.

Secure Flight: TSA Could Take Additional Steps to Strengthen Privacy Oversight Mechanisms

Number: [GAO-14-647](#)

Date: September 9, 2014

Summary: The Transportation Security Administration (TSA) has taken steps to implement several of the privacy oversight mechanisms it planned to establish when Secure Flight implementation began in 2009, but additional actions could allow TSA to sustain and strengthen its efforts. Overall, TSA has implemented mechanisms to identify privacy implications associated with program operations and address them as necessary. For example, TSA has regularly updated privacy documents to address changes in the Secure Flight program. TSA has also implemented privacy training for new Secure Flight staff, and all Department of Homeland Security (DHS) employees receive annual privacy training. However, existing Secure Flight staff do not receive job-specific privacy refresher training consistent with Office of Management and Budget (OMB) requirements. Providing job-specific privacy refresher training could further strengthen Secure Flight's protection of personally identifiable information (PII). TSA also documents some aspects of its Secure Flight privacy oversight mechanisms, such as scheduled destructions of passenger data and reviews of planned changes to the Secure Flight system. However, TSA does not have a mechanism to comprehensively document and track key privacy-related issues and decisions that arise through the development and use of Secure Flight—a mechanism TSA planned to develop when Secure Flight was implemented in 2009. Comprehensively documenting and tracking key privacy-related issues and decisions, in accordance with federal internal control standards, could help TSA ensure that these decisions are carried into the future in the event of a change in personnel.

The DHS Traveler Redress Inquiry Program (DHS TRIP) affords passengers who may have been incorrectly matched to or listed on high-risk lists based on the Terrorist Screening Database (TSDB)—the U.S. government's consolidated list of known and suspected terrorists—an opportunity to seek redress. Passengers who, through the redress process, are determined to have been misidentified to a TSDB-based high-risk list are added to the TSA Cleared List, which allows them to be cleared (not identified as high risk) nearly 100 percent of time. The DHS TRIP process also allows passengers determined to have been improperly included on a TSDB-based list (mislisted) to be removed, minimizing the likelihood they will be identified as matches during future travels. Although DHS TRIP is not able to provide redress for passengers who may have been misidentified to high-risk, rules-based lists—TSA's lists of passengers who meet intelligence-driven criteria indicating they may pose a greater security risk—according to TSA officials, TSA procedures for using the lists mitigate impacts on these passengers. In fiscal year 2013, DHS TRIP began working to reduce processing time for its redress and appeals cases. In fiscal year 2014, DHS TRIP reduced its target for one of its key performance indicators—average number of days for DHS TRIP redress cases to be closed—from 93 to 78 days—and, for the first time, established a performance goal for the appeals process of 92 days. For fiscal years 2011 through 2013, the average total processing time for an appeals case was about 276 days. DHS TRIP plans to periodically review its progress in achieving its appeals performance goal and determine by February 2015 whether further changes to the appeals process are warranted.

GAO recommends that TSA provide job-specific privacy refresher training for Secure Flight staff and develop a mechanism to document and track key Secure Flight privacy issues and decisions.

DHS OIG Reports

TSA's SPOT Program and Initial Lessons from the LAX Shooting

Number: [Testimony](#)

Date: November 14, 2013

Summary: Since the Screening of Passengers by Observation Techniques program began in FY 2007, TSA data indicate that the program has expanded from \$20 million to \$205 million in expended costs and the number of airports with the program has grown from 42 to 176. However, TSA has not implemented a strategic plan to ensure the program's success. TSA did not: (1) assess the effectiveness of the program, (2) have a comprehensive training program, (3) ensure outreach to its partners, or (4) have a financial plan. As a result, TSA could not ensure that passengers at United States airports were screened objectively, show that the program was cost-effective, or reasonably justify the program's expansion. In FY 2012, TSA's Behavior Detection and Analysis Division developed a draft strategic plan that included a statement of mission, goals, and objectives. However, the plan had not been approved and implemented at the time of our audit.

Examining TSA's Cadre of Criminal Investigators

Number: [Testimony](#)

Date: January 28, 2014

Summary: OOI conducts inspections, internal reviews, and covert testing to ensure the effectiveness and efficiency of TSA's operations and administrative activities, and to identify vulnerabilities in TSA security systems. Additionally, the office carries out internal investigations of the TSA workforce to ensure its integrity. We conducted an audit of this office to determine whether it is efficient and effective in its efforts to enhance transportation security.

We determined that OOI did not operate efficiently. Specifically, the office did not use its staff and resources efficiently to conduct cost-effective inspections, internal reviews, and covert testing. OOI employed personnel classified as criminal investigators, even though their primary duties may not have been criminal investigations as required by Federal law and regulations. These employees received premium pay and other costly benefits, although other employees were able to perform the same work at a lower cost. Additionally, the office did not properly plan its work and resource needs, track project costs, or measure performance effectively. Quality controls were not sufficient to ensure that inspections, internal reviews, and covert testing complied with accepted standards; that staff members were properly trained; and that work was adequately reviewed. Finally, the office could not always ensure that other TSA offices acted on its recommendations to improve operations.

As a result of these issues with the office's cost-effectiveness and quality controls over its work products, TSA was not as effective as it could have been, and management may not be able to rely on the office's work. Additionally, OOI may not have fully accomplished its mission to identify and address transportation security vulnerabilities. With the appropriate classification and training of staff and better use of resources, the office could improve the quality of its work. The

appropriate number of reclassifications and more precise cost savings cannot be determined without an objective and comprehensive review of position classifications. If TSA does not make any changes to the number of criminal investigator positions in OOI, we estimate that it will cost as much as \$17.5 million over 5 years for premium Law Enforcement Availability Pay (LEAP). OOI could realize further savings in training, travel, supplies, and other special employment benefits, including statutory early retirement, if its personnel classified as criminal investigators were reclassified to noncriminal investigator positions.

TSA's Management of Secure 1000SP Advanced Imaging Technology Units

Number: [OIG-14-138](#)

Date: September 10, 2014

Summary: In 2007, TSA began deploying advanced imaging technology to screen airline passengers for weapons, explosives, and other concealed objects. In 2009 and 2010, TSA used American Recovery and Reinvestment Act funds to purchase 251 Secure 1000SP advanced imaging technology units from Rapiscan Systems. By June 2013, TSA had removed the units from service because the company could not develop enhanced software to enable the units to comply with the privacy requirements of the FAA Modernization and Reform Act of 2012. Rapiscan Systems assumed all costs associated with their removal and storage.

In May 2013, Representative Bennie Thompson requested that we review TSA's management of its advanced imaging technology inventory. Specifically, Mr. Thompson requested that we review the removal and potential redistribution of the noncompliant units, and related costs.

TSA purchased 251 units and technical support services for \$41,653,702. However, TSA was unable to determine the deployment cost for the units because the task orders used do not segregate individual costs. TSA complied with property transfer regulations for the 251 units. As of August 29, 2014, TSA transferred 165 units to other federal, state, and local law enforcement agencies.

During our fieldwork, we determined that TSA and Rapiscan Systems may not have sanitized sensitive security information from one unit's computer system prior to donating it to a state agency. We promptly informed TSA program officials about the possible security concern. One week later, a TSA official traveled to the state agency's warehouse and removed the unit's hard drive.

Vulnerabilities Exist in TSA's Checked Baggage Screening Operations

Number: [OIG-14-142](#)

Date: September 16, 2014

Summary: The Transportation Security Administration (TSA) is responsible for protecting the Nation's transportation systems to ensure freedom of movement for people and commerce. As part of its mission, TSA screens checked baggage to deter, detect, and prevent the carriage of any prohibited items, such as explosives and incendiaries, onboard passenger commercial aircraft. TSA primarily relies on its screening workforce and two types of equipment to screen checked baggage—explosives detection systems and explosives trace detection.

Through covert testing conducted at domestic airports, we determined whether Transportation Security Officers were following established policies and procedures to prevent threat items from being placed onto commercial aircraft. We also determined the operational effectiveness of TSA's

checked baggage screening technology. We identified vulnerabilities in this area caused by human and technology-based failures. We also determined that TSA does not have a process in place to assess or identify the cause for equipment-based test failures or the capability to independently assess whether deployed explosive detection systems are operating at the correct detection standards. The compilation of the number of tests conducted, the names of airports tested, and test results are classified, or designated as Sensitive Security Information. According to TSA, the component spent \$540 million for checked baggage screening equipment and \$11 million for training since 2009. Despite that investment, TSA has not improved checked baggage screening since our last report in 2009. We made five recommendations that, when implemented, should increase the effectiveness of the checked baggage screening process.

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

GAO Reports

Critical Infrastructure Protection: Observations on DHS Efforts to Implement and Manage its Chemical Security Program

Number: [GAO-14-608T](#) (Testimony)

Date: May 14, 2014

Summary: In managing its Chemical Facility Anti-Terrorism Standards (CFATS) program, the Department of Homeland Security (DHS) has a number of efforts underway to identify facilities that are covered by the program, assess risk and prioritize facilities, review and approve facility security plans, and inspect facilities to ensure compliance with security regulations.

- **Identifying facilities.** DHS has begun to work with other agencies to identify facilities that should have reported their chemical holdings to CFATS, but may not have done so. DHS initially identified about 40,000 facilities by publishing a CFATS rule requiring that facilities with certain types and quantities of chemicals report certain information to DHS. However, a chemical explosion in West, Texas last year demonstrated the risk posed by chemicals covered by CFATS. Subsequent to this incident, the President issued Executive Order 13650 which was intended to improve chemical facility safety and security in coordination with owners and operators. Under the executive order, a federal working group is sharing information to identify additional facilities that are to be regulated under CFATS, among other things.
- **Assessing risk and prioritizing facilities.** DHS has begun to enhance its ability to assess risks and prioritize facilities. DHS assessed the risks of facilities that reported their chemical holdings in order to determine which ones would be required to participate in the program and subsequently develop site security plans. GAO's April 2013 report found weaknesses in multiple aspects of the risk assessment and prioritization approach and made recommendations to review and improve this process. In February 2014, DHS officials told us they had begun to take action to revise the process for assessing risk and prioritizing facilities.

- **Reviewing security plans.** DHS has also begun to take action to speed up its reviews of facility security plans. Per the CFATS regulation, DHS is to review security plans and visit the facilities to make sure their security measures meet the risk-based performance standards. GAO's April 2013 report found a 7- to 9-year backlog for these reviews and visits, and DHS has begun to take action to expedite these activities. As a separate matter, one of the performance standards—personnel surety, under which facilities are to perform background checks and ensure appropriate credentials for personnel and visitors as appropriate—is being developed. Of the facility plans DHS had reviewed as of February 2014, it conditionally approved these plans pending final development of the personal surety performance standard. According to DHS officials, it is unclear when the standard will be finalized.
- **Inspecting to verify compliance.** In February 2014, DHS reported it had begun to perform inspections at facilities to ensure compliance with their site security plans. According to DHS, these inspections are to occur about 1 year after facility site security plan approval. Given the backlog in plan approvals, this process has started recently and GAO has not yet reviewed this aspect of the program.

Chemical Safety: Actions Needed to Improve Federal Oversight of Facilities with Ammonium Nitrate

Number: [GAO-14-274](#)

Date: May 19, 2014

Summary: Federal data provide insight into the number of facilities in the United States with ammonium nitrate but do not provide a complete picture because of reporting exemptions and other data limitations. The Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA) do not require facilities to report their ammonium nitrate holdings. The Department of Homeland Security (DHS) requires facilities with certain quantities of ammonium nitrate to report their holdings for security purposes. While the total number of facilities in the United States with ammonium nitrate is unknown, as of August 2013, at least 1,300 facilities in 47 states reported to DHS that they had reportable quantities of ammonium nitrate. Federal law also requires certain facilities to report their ammonium nitrate holdings to state and local authorities for emergency planning purposes, but these data are not routinely shared with federal agencies. According to EPA, states are not required to report these data to federal agencies, and each state determines how to share its data. As part of an Executive Order on Improving Chemical Facility Safety and Security issued in August 2013, federal agencies are exploring options for improving data sharing, but this work is not yet complete.

International chemical safety guidance suggests authorities should provide facilities information on how regulatory requirements can be met and periodically inspect them. GAO reviewed approaches to overseeing facilities with ammonium nitrate in Canada, France, Germany, and the United Kingdom, selected in part based on recommendations from chemical safety experts. According to foreign officials and government documents, these countries require facilities with specified quantities of ammonium nitrate to assess its risk and develop plans or policies to prevent chemical accidents. For example, Canadian officials said facilities with 22 tons or more of ammonium nitrate are required to complete a risk assessment and an emergency plan. Some countries' storage requirements also restrict the use of wood to store ammonium nitrate.

GAO is recommending that federal agencies improve data sharing, OSHA and EPA consider revising their related regulations to cover ammonium nitrate, and OSHA conduct outreach to the fertilizer industry and target high risk facilities for inspection. DHS, EPA, and OSHA agreed with GAO's recommendations and suggested technical changes, which GAO incorporated as appropriate.

Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources

Number: [GAO-14-293](#)

Date: June 12, 2014

Summary: GAO found that challenges exist in reducing the security risks faced by licensees using high-risk industrial radiological sources. Specifically, licensees face challenges in (1) securing mobile and stationary sources and (2) protecting against an insider threat. Regarding mobile sources, their portability makes them susceptible to theft or loss, as the size of some of these sources is small enough for them to be easily concealed. The most common mobile source is contained in a device called a radiography camera. GAO identified four incidents from 2006 to 2012 where such cameras that use high-risk sources to test pipeline welds were stolen. Licensees also face challenges in determining which employees are suitable for trustworthiness and reliability (T&R) certification to have unescorted access to high-risk radiological sources. GAO found two cases where employees were granted unescorted access, even though each had extensive criminal histories, and one had been convicted for terroristic threats, which include a range of violent threats.

Federal agencies responsible for securing radiological sources—including NRC, the National Nuclear Security Administration (NNSA), and the Department of Homeland Security (DHS)—have taken steps to improve the security of industrial radiological sources. However, GAO found that although the agencies have been meeting quarterly to discuss, among other things, radiological security, this mechanism did not always help them collaborate and draw on each agency's expertise during research, development, and testing of a new technology for a mobile source tracking device. By not collaborating consistently, the agencies have missed opportunities to leverage resources and expertise in developing this new technology to track radiological sources. This technology could aid in the timely recovery of a lost or stolen radiological source and support the agencies' common mission. As GAO has previously reported, when responsibilities cut across more than one federal agency—as they do for securing industrial radiological sources—it is important for agencies to work collaboratively to deliver results more efficiently and in a way that is consistent with the federal government's multiple demands and limited resources.

GAO recommends, among other things, that NRC assess the T&R process to determine if it provides reasonable assurance against insider threats. In addition, GAO recommends that NNSA, NRC, and DHS review their collaboration mechanism for opportunities to enhance it, especially in the development of new technologies. NRC generally agreed with GAO's recommendations, and NNSA agreed with the one recommendation directed to it. DHS did not comment on the report.

Biosurveillance: Observations on the Cancellation of BioWatch Gen-3 and Future Considerations for the Program**Number:** [GAO-14-267T](#) (Testimony)**Date:** June 10, 2014

Summary: In September 2012, GAO reported that the Department of Homeland Security (DHS) approved the Office of Health Affairs (OHA) acquisition of a next generation biosurveillance technology (Gen-3) in October 2009 without fully following its acquisition processes. To help ensure DHS based its acquisition decisions on reliable performance, cost, and schedule information, GAO recommended that before continuing the Gen-3 acquisition, DHS reevaluate the mission need and alternatives. DHS concurred with the recommendation and in 2012 decided to reassess mission needs and conduct a more robust AoA. Following the issuance of the AoA in December 2013, DHS decided in April 2014 to cancel Gen-3 acquisition and move the technology development back to the Science and Technology Directorate (S&T). According to DHS's acquisition decisions memorandum, the AoA did not confirm an overwhelming benefit to justify the cost of a full technology switch to Gen-3. Moreover, DHS officials said the decision to cancel the Gen-3 acquisition was a cost-effectiveness measure, because the system was going to be too costly to develop and maintain in its current form.

GAO's prior work on DHS research and development (R&D) highlights challenges DHS may face in shifting efforts back to S&T and acquiring another biodetection technology. In September 2012, GAO reported that while S&T had dozens of technology transition agreements with DHS components, none of these had yet resulted in a technology developed by S&T being used by a component. At the same time, other DHS component officials GAO interviewed did not view S&T's coordination practices positively. GAO recommended that DHS develop and implement policies and guidance for defining and overseeing R&D at the department that includes a well-understood definition of R&D that provides reasonable assurance that reliable accounting and reporting of R&D resources and activities for internal and external use are achieved. S&T agreed with GAO's recommendations and efforts to address them are ongoing. Addressing these coordination challenges could help to ensure that S&T's technology development efforts meet the operational needs of OHA.

Cancellation of the Gen-3 acquisition also raises potential challenges that the currently deployed Gen-2 system could face going forward. According to DHS officials, DHS will continue to rely on its Gen-2 system as an early indicator of an aerosolized biological attack. However, in 2011, National Academy of Sciences raised questions about the effectiveness of the currently deployed Gen-2 system. While Gen-2 has been used in the field for over a decade, the National Academy of Sciences reported that information about the technical capabilities of the system, including the limits of detection, is limited. In April 2014, DHS officials also indicated that they will soon need to replace laboratory equipment of the currently deployed Gen-2 system and readjust life cycle costs since there will be no Gen-3 technology to replace it.

Combating Nuclear Smuggling: Past Work and Preliminary Observations on Research and Development at the Domestic Nuclear Detection Office**Number:** [GAO-14-783T](#) (Testimony)**Date:** July 29, 2014**Summary:** GAO has reported on the Department of Homeland Security's (DHS) Domestic Nuclear Detection Office's (DNDO) since 2006. GAO has identified challenges and made recommendations in the following areas:

- **DNDO's efforts to develop the Global Nuclear Detection Architecture (GNDA):** In 2008, GAO recommended that DHS develop a strategic plan to guide the development of the GNDA, a framework for 74 independent programs, projects, or activities to detect and interdict nuclear smuggling. In 2010, DHS issued a plan and GAO reviewed this plan and found that it generally addressed GAO's recommendations.
- **DNDO's efforts to replace radiation detection equipment:** GAO has found challenges in DNDO's efforts to develop and deploy radiation portal monitors, which scan for nuclear or radiological materials at ports of entry. GAO has made several recommendations throughout the history of these efforts, and DNDO has taken actions that have generally been responsive.
- **DHS's efforts to coordinate research and development (R&D) across the agency.** In 2012 and 2013, GAO made recommendations to help DHS oversee its R&D investments and efforts, and in particular its border and maritime R&D efforts. GAO's recommendations focused on strengthening coordination and defining R&D across the agency. DHS concurred with GAO's recommendations and described actions it plans to take in response.

Preliminary observations from GAO's ongoing review are that DNDO has taken steps to manage R&D and assess project outcomes, but that it may not be able to demonstrate how agency investments align with critical mission needs. DNDO officials told GAO that they discuss how research projects may contribute to critical mission needs but that they do not document these discussions. Once research projects are complete, DNDO officials told GAO they evaluate the success of individual research projects, but DNDO does not have a systematic approach to ensure its overall R&D investments address gaps in the GNDA. As a result, DNDO may not be able to demonstrate to key stakeholders—including oversight organizations and potential users of new technologies—that its R&D investments are aligned with critical mission needs.

GAO's ongoing work indicates that DNDO officials have taken some steps to coordinate R&D efforts internally, with other federal agencies, and with end users, but preliminary analysis shows that not all of DNDO's end users are satisfied with DNDO's communication. DNDO directorates work closely to identify critical mission needs, and DNDO collaborates with other federal research agencies to leverage expertise. However, DNDO's end users varied in their satisfaction with DNDO's efforts to coordinate with them. Officials from two end user agencies told GAO that coordination was working well; however, officials from the largest end user agency stated that they were generally dissatisfied with DNDO's coordination because DNDO's research directorate does not provide them information directly and, in some cases, found that project requirements would not meet the agency's operational needs. This is consistent with GAO's 2010 finding that inadequate communication caused DNDO to pursue scanning technology that would not meet the operational requirements of the end user if it were deployed.

DHS OIG Reports

Domestic Nuclear Detection Office Has Taken Steps to Address Insider Threat, but Challenges Remain

Number: [OIG-14-113](#)

Date: July 21, 2014

Summary: Steps are underway to address and mitigate the insider risk at DNDO. Specifically, the Department of Homeland Security (DHS) Acting Under Secretary of Intelligence and Analysis established an Insider Threat Task Force to develop a program to address the risk of insider threats for DHS, including DNDO. In addition, the DHS Office of Intelligence and Analysis has detailed a counterintelligence officer to DNDO to help mitigate espionage-related insider risks. The DHS Office of Intelligence and Analysis routinely briefs DNDO on counterintelligence awareness, including insider threat indicators. In addition, DNDO provides security awareness training to its employees and contractors regarding security-related topics that could help prevent or detect the insider risk. In September 2013, the DHS Office of the Chief Security Officer began a comprehensive vulnerability assessment of DNDO assets, which includes identifying insider risks and vulnerabilities. The DHS Security Operations Center monitors DNDO information systems and networks to respond to potential insider based incidents. Finally, the DHS Special Security Programs Division handles and investigates security incidents, including those types attributed to malicious insiders.

Additional steps to address the insider risk at DNDO are required. Specifically, DNDO needs to implement insider threat procedures, upon receipt of policy issued by the DHS Office of the Chief Information Officer (OCIO) that defines roles and responsibilities for addressing insider risks to unclassified networks and systems. DNDO also needs to provide documentation that clearly shows the effectiveness of controls or processes in place to detect and respond to unauthorized data exfiltration from DNDO unclassified information technology assets via email services provided by the DHS OCIO.

We are making five recommendations that, if implemented, should strengthen DNDO's security posture against the risk posed by trusted insiders.

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

GAO Reports

Federal Protective Service: Protecting Federal Facilities Remains a Challenge

Number: [GAO-14-623T](#) (Testimony)

Date: May 21, 2014

Summary: The Federal Protective Service continues to face challenges ensuring that contract guards have been properly trained and certified before being deployed to federal facilities around the country. In September 2013 GAO reported that providing training for active shooter scenarios

and screening access to federal facilities poses a challenge for FPS. Without ensuring that all guards receive training on how to respond to active-shooter incidents at federal facilities, FPS has limited assurance that its guards are prepared for this threat. GAO was unable to determine the extent to which FPS's guards have received active-shooter response and screener training, in part, because FPS lacks a comprehensive and reliable system for guard oversight. GAO also found that FPS continues to lack effective management controls to ensure its guards have met its training and certification requirements.

Assessing risk at federal facilities remains a challenge for FPS. GAO found in 2012 that federal agencies pay FPS millions of dollars to assess risk at their facilities, but FPS is not assessing risks in a manner consistent with federal standards. In March 2014, GAO found that this is still a challenge for FPS and several other agencies. The Interagency Security Committee's (ISC) *Risk Management Process for Federal Facilities* standard requires federal agencies to develop risk assessment methodologies that, among other things, assess the threat, vulnerability, and consequence to undesirable events. Risk assessments help decision-makers identify and evaluate security risks and implement protective measures. Instead of conducting risk assessments, FPS uses an interim vulnerability assessment tool, referred to as the Modified Infrastructure Survey Tool (MIST) to assess federal facilities until it develops a longer-term solution. However, MIST does not assess consequence (the level, duration, and nature of potential loss resulting from an undesirable event). Three of the four risk assessment experts GAO spoke with generally agreed that a tool that does not estimate consequences does not allow an agency to fully assess risks. Thus, FPS has limited knowledge of the risks facing about 9,600 federal facilities around the country. FPS officials stated that consequence information in MIST was not part of the original design, but they are exploring ways to incorporate it.

Since fiscal year 2010, GAO has made 31 recommendations to improve FPS's contract guard and risk assessment processes, of which 6 were implemented, 10 are in process, and 15 have not been implemented.

DHS OIG Reports

The Chemical Facility Anti-Terrorism Standards Authorization and Accountability Act of 2014

Number: [Testimony](#)

Date: February 27, 2014

Summary: In December 2011, a limited distribution internal memorandum, prepared by Infrastructure Security Compliance Division (ISCD) management, was leaked to news media. The document disclosed allegations of employee misconduct and inadequate performance, as well as misuse of funds and ineffective hiring within the Department of Homeland Security's (DHS) Chemical Facility Anti - Terrorism Standards (CFATS) Program. In February 2012, former Chairman Lungren, of the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, requested that we review these issues. In April 2012, Ranking Member Waxman, of the House Committee on Energy and Commerce, also requested that we review the challenges facing this program.

In March 2013, we issued a report, Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti - Terrorism Standards Program, OIG-13-55. We reviewed whether: (1) management controls are in place and operational to ensure that the CFATS Program is not mismanaged; (2) National Protection and Programs Directorate (NPPD) and ISCD leadership misrepresented program progress; and (3) nonconforming opinions of program personnel have been suppressed or met with retaliation.

ISCD addressed some issues contained in the December 2011 memorandum; however, challenges remain. Misinterpretations of congressional intent may have put unnecessary pressure on ISCD to develop and implement the CFATS Program, resulting in poor management oversight and internal controls, personnel issues, and missed milestones.

In our March 2013 report, we made 24 recommendations to correct program deficiencies and attain intended program results and outcomes. Currently, 12 report recommendations are resolved and open, and 12 recommendations are closed.

Mission 2: Secure and Manage Our Borders

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

GAO Reports

Maritime Security: Progress and Challenges in Key DHS Programs to Secure the Maritime Borders

Number: [GAO-14-196T](#) (Testimony)

Date: November 19, 2013

Summary: GAO's prior work has identified several key factors important to secure the maritime borders. The Department of Homeland Security (DHS) and its components have made progress (e.g., coordinating with partners), and in some cases also experienced challenges with their related maritime security programs.

- **Maintaining robust maritime domain awareness.** It is critical that federal agencies maintain maritime domain awareness--the understanding of anything associated with the global maritime environment that could adversely affect the security, safety, economy, or environment of the United States. The U.S. Coast Guard has developed systems--including information-sharing and vessel-tracking systems--to enhance maritime domain awareness. GAO's prior work has found that the Coast Guard has made progress in developing its systems, but that it also experienced some challenges.
- **Assessing risks coming from foreign ports.** The security of maritime borders also depends upon security at foreign ports where cargo bound for the United States originates. U.S. Customs and Border Patrol (CBP) and the Coast Guard have developed models to assess the risks of foreign ports, foreign vessels entering U.S. ports, and the cargo carried by these vessels from these ports. In September 2013, GAO found that CBP has taken steps to enhance the security of U.S.-bound cargo, but CBP does not periodically assess the supply chain security risks from foreign ports that ship cargo to the United States. GAO recommended that CBP periodically assess the supply chain security risks from these ports. DHS concurred with GAO's recommendation and reported that it planned to take actions to address it.
- **Conducting maritime surveillance, interdiction, and security operations.** Along the coasts and in ports, maritime surveillance, interdiction, and operations are conducted to ensure the security of the maritime borders. For example, CBP's Office of Air and Marine is to provide maritime surveillance and interdiction capabilities. In March 2012, GAO found that the office did not meet its national performance goal and did not provide higher rates of support in locations designated as high priority. GAO made recommendations to help ensure that the office's assets and personnel are best positioned to effectively meet mission needs and address threats, among other things. DHS concurred and reported that it planned to take action to address the recommendations by the end of March 2014.
- **Measuring performance. In securing our maritime borders, DHS and its component agencies have faced challenges in developing meaningful performance measures.** For example, GAO's prior work found that they have experienced challenges collecting complete, accurate, and reliable data; among other things. In January 2011, GAO reported

that both CBP and the Coast Guard tracked the frequency of illegal seafarer incidents at U.S. seaports, but the records of these incidents varied considerably between the two component agencies and between the agencies' field and headquarters units. GAO made a recommendation to improve the accuracy of DHS data, and DHS concurred and has made progress in addressing the recommendation.

Maritime Security: DHS Could Benefit from Tracking Progress in Implementing the Small Vessel Security Strategy

Number: [GAO-14-32](#)

Date: October 31, 2013

Summary: The Department of Homeland Security (DHS) and its components--such as the U.S. Coast Guard and Customs and Border Protection (CBP)--have started or completed initiatives to address small vessel security risks, but DHS is not tracking the progress being made to address action items in the *Small Vessel Security Strategy (SVSS) Implementation Plan*. "Small vessels" are characterized as any watercraft--regardless of method of propulsion--less than 300 gross tons, and used for recreational or commercial purposes. DHS component officials GAO met with identified examples of key initiatives that they have completed or have under way to enhance small vessel security, including an initiative to help CBP better track small vessels arriving from foreign locations and another to assist the Coast Guard in assessing and monitoring small vessel launch sites. Although the *SVSS Implementation Plan* states that DHS is to assess and update the plan, DHS has not determined the progress its components and other relevant stakeholders--such as the Department of Defense--are making in completing the action items and has no current plans to do so. DHS officials stated that this is due, in part, to budget constraints that make this a low priority. DHS officials stated that updating the *SVSS Implementation Plan* would be valuable, and doing so is particularly important since more than one component could be responsible for action items in the plan. Accordingly, by systematically gathering information from its components and other relevant stakeholders to regularly update the progress they are making in addressing the action items in the plan, DHS could help prioritize initiatives given constrained budgets and better identify successes and lessons learned, among other things.

GAO recommends that DHS regularly update the progress its components and other relevant stakeholders are making in addressing action items in the *SVSS Implementation Plan*.

Border Security: DHS's Efforts to Modernize Key Enforcement Systems Could be Strengthened

Number: [GAO-14-62](#)

Date: December 5, 2013

Summary: Customs and Border Protection (CBP) has defined the scope for its TECS (not an acronym) modernization (TECS Mod) program, but its schedule and cost continue to change; while Immigration and Customs Enforcement (ICE) is overhauling the scope, schedule, and cost of its program after discovering that its initial solution is not technically viable. CBP's \$724 million program intends to modernize the functionality, data, and aging infrastructure of legacy TECS and move it to DHS's data centers. CBP plans to develop, deploy, and implement these capabilities between 2008 and 2015. To date, CBP has deployed functionality to improve its secondary inspection processes to air and sea ports of entry and, more recently, to land ports of entry in 2013. However, CBP is in the process of revising its schedule baseline for the second time in under a year. Further, portions of CBP's schedule remain undefined and the program does not have a fully

developed master schedule. These factors increase the risk of CBP not delivering TECS Mod by its 2015 deadline. Regarding ICE's \$818 million TECS Mod program, it is redesigning and replanning its program, having determined in June 2013 that its initial solution was not viable and could not support ICE's needs. As a result, ICE halted development and is now assessing design alternatives and will revise its schedule and cost estimates. Program officials stated the revisions will be complete in December 2013. Until ICE completes the replanning effort, it is unclear what functionality it will deliver, when it will deliver it, or what it will cost to do so, thus putting it in jeopardy of not completing the modernization by its 2015 deadline.

CBP and ICE have managed many risks in accordance with some leading practices, but they have had mixed results in managing requirements for their programs. In particular, neither program identified all known risks and escalated them for timely management review. Further, CBP's guidance defines key practices associated with effectively managing requirements, but important requirements development activities were underway before these practices were established. ICE, meanwhile, operated without requirements management guidance for years, and its requirements activities were mismanaged as a result.

The Department of Homeland Security's (DHS) governance bodies have taken actions to oversee the two TECS Mod programs that are generally aligned with leading practices. Specifically, DHS's governance bodies have monitored TECS Mod performance and progress and have ensured that corrective actions have been identified and tracked. However, the governance bodies' oversight has been based on sometimes incomplete or inaccurate data, and therefore the effectiveness of these efforts is limited. Until these governance bodies base their performance reviews on timely, complete, and accurate data, they will be constrained in their ability to effectively provide oversight.

GAO is recommending DHS improve its efforts to manage requirement and risk, as well as its governance of the TECS Mod programs.

Arizona Border Surveillance Technology Plan: Additional Actions Needed to Strengthen Management and Assess Effectiveness

Number: [GAO-14-368](#)

Date: March 12, 2014

Summary: The Department of Homeland Security's (DHS) U.S. Customs and Border Protection's (CBP) schedules and Life-cycle Cost Estimates for the Arizona Border Surveillance Technology Plan (the Plan) reflect some, but not all, best practices. Scheduling best practices are summarized into four characteristics of reliable schedules—comprehensive, well-constructed, credible, and controlled (i.e., schedules are periodically updated and progress is monitored). GAO assessed CBP's schedules as of March 2013 for the three highest-cost programs that represent 97 percent of the Plan's estimated cost. GAO found that schedules for two of the programs at least partially met each characteristic (i.e., satisfied about half of the criterion), and the schedule for the other program at least minimally met each characteristic (i.e., satisfied a small portion of the criterion), as shown in the table below.

Further, CBP has not developed an Integrated Master Schedule for the Plan in accordance with best practices. Rather, CBP has used the separate schedules for each program to manage implementation of the Plan, as CBP officials stated that the Plan contains individual acquisition programs rather than integrated programs. However, collectively these programs are intended to

provide CBP with a combination of surveillance capabilities to be used along the Arizona border with Mexico, and resources are shared among the programs. Developing and maintaining an Integrated Master Schedule for the Plan could help provide CBP a comprehensive view of the Plan and help CBP better understand how schedule changes in each individual program could affect implementation of the overall Plan.

CBP did not fully follow key aspects of DHS's acquisition management guidance for the Plan's three highest-cost programs. For example, CBP plans to conduct limited testing of the highest-cost program—the Integrated Fixed Tower (IFT: towers with cameras and radars)—to determine its mission contributions, but not its effectiveness and suitability for the various environmental conditions, such as weather, in which it will be deployed.

CBP has identified mission benefits for technologies under the Plan, but has not yet developed performance metrics. CBP has identified such mission benefits as improved situational awareness and agent safety. Further, a DHS database enables CBP to collect data on asset assists, defined as instances in which a technology, such as a camera, or other asset, such as a canine team, contributed to an apprehension or seizure, that in combination with other relevant performance metrics or indicators, could be used to better determine the contributions of CBP's surveillance technologies and inform resource allocation decisions. However, CBP is not capturing complete data on asset assists, as Border Patrol agents are not required to record and track such data.

GAO recommends that CBP, among other things, apply scheduling best practices, develop an integrated schedule, verify Life-cycle Cost Estimates, revise the IFT test plan, and require tracking of asset assist data. As discussed in this report, GAO continues to believe in the need for a schedule and a revised test plan.

Maritime Security: Progress and Challenges with Selected Port Security Programs

Number: [GAO-14-636T](#) (Testimony)

Date: June 4, 2014

Summary: GAO's prior work has shown that the Department of Homeland Security (DHS) and its component agencies—particularly the Coast Guard and Customs and Border Protection (CBP)—have made substantial progress in three key areas of port security since the September 11, 2001 terrorist attacks (9/11), but some challenges remain.

- **Maritime domain awareness and information sharing.** DHS agencies along with other port partners have taken actions to enhance visibility over the maritime domain and facilitate cooperation among partners by collecting, assessing, and sharing key information. However, some challenges remain in implementing the tools necessary to maintain this focus and increase coordination among stakeholders. For example, in multiple reports since 2011, GAO found the Coast Guard's weak management of technology acquisitions—that were focused on enhancing maritime awareness and increasing communication among partners—resulted in these acquisitions not fully achieving their intended purposes. DHS concurred with GAO's recommendations for addressing these weaknesses.
- **Security in domestic ports.** Since 9/11, DHS components have taken a wide variety of actions to better secure domestic ports. For example, the Coast Guard has assessed risks to cruise ships in accordance with DHS guidance and is providing escorts for high-risk vessels such as cruise ships and ferries while CBP is reviewing passenger and crew data to target

inspections. In addition, since 2002, the Federal Emergency Management Agency (FEMA) has provided almost \$2.9 billion in federal funding through the Port Security Grant Program (PSGP) to help defray the cost of implementing security efforts in many ports and has established measures to improve the administration of the PSGP. However, in 2014 FEMA stated that it is unable—due to resource constraints—to annually measure reduced vulnerability attributed to enhanced PSGP-funded security measures. Meanwhile, the Transportation Security Administration (TSA) and the Coast Guard have been administering a program requiring maritime workers to obtain a biometric identification card to gain access to certain facilities. However, in 2011, GAO recommended that DHS assess internal controls to identify actions needed to address, among other things, weaknesses governing enrollment and background checks. As of March 2014 this action had not been completed.

- **Protection of the global supply chain.** DHS agencies, especially CBP, have taken steps to enhance the security of the global supply chain—particularly for cargo bound for the United States. Efforts have focused on assessing and mitigating cargo risk before it enters U.S. ports by better targeting and scanning cargo, and establishing security partnerships with the foreign countries and companies that ship cargo to the United States. However, in multiple reports since 2005, GAO found that DHS programs focused on protecting the global supply chain have been implemented with varying degrees of success and that many would benefit from the DHS agencies conducting further assessments of the programs, among other things. GAO has made recommendations to address these issues and DHS has concurred or generally concurred with most of these recommendations and has taken actions to address many of them.

Coast Guard: Resources Provided for Drug Interdiction Operations in the Transit Zone, Puerto Rico, and the U.S. Virgin Islands

Number: [GAO-14-527](#)

Date: June 16, 2014

Summary: The Coast Guard provided varying levels of resources for drug interdiction operations in the “transit zone”—the area from South America through the Caribbean Sea and the eastern Pacific Ocean that is used to transport illicit drugs to the United States—during fiscal years 2009 through 2013, and generally did not meet its performance targets for several reasons. The number of cutter days, aircraft hours, and law enforcement detachment days the Coast Guard provided for drug interdiction operations in the transit zone varied during fiscal years 2009 through 2012, and then sharply declined in fiscal year 2013. During fiscal years 2009 through 2013, the Coast Guard met targets for its primary drug interdiction mission performance measure—the removal rate of cocaine from noncommercial vessels in the transit zone—once, in fiscal year 2013. Coast Guard officials cited the declining readiness of its aging vessels, delays in the delivery of replacement vessels, and sequestration as factors affecting Coast Guard resource deployments and the ability to meet its drug interdiction mission performance targets.

In support of a Department of Homeland Security (DHS) effort to address the increased violent crime associated with illicit drug smuggling into Puerto Rico and the U.S. Virgin Islands, the Coast Guard has increased vessel and aircraft operations for drug interdiction efforts in these territories by reallocating resources from elsewhere in the Coast Guard. According to Coast Guard officials, these additional resources are drawn from other missions, such as alien migrant interdiction. Beginning in September 2012, the Coast Guard implemented a surge operation to provide additional vessels and aircraft to regularly patrol Puerto Rico and the U.S. Virgin Islands. According to Coast

Guard officials, the increased vessel and aircraft deployments have since become the new baseline level of resources to be provided for drug interdiction operations there. According to Coast Guard data, the number of vessel hours spent conducting drug interdiction operations in these territories more than tripled from fiscal years 2009 through 2013. Similarly, the number of maritime patrol aircraft hours spent conducting drug interdiction operations in the territories increased—from about 150 flight hours in fiscal year 2011 to about 1,000 hours in fiscal year 2013.

Border Security: Opportunities Exist to Strengthen Collaborative Mechanism along the Southwest Border

Number: [GAO-14-494](#)

Date: June 27, 2014

Summary: The Department of Homeland Security (DHS) has coordinated border security efforts using collaborative mechanisms in Arizona and South Texas, specifically (1) the Joint Field Command (JFC), which has operational control over all U.S. Customs and Border Protection (CBP) resources in Arizona; (2) the Alliance to Combat Transnational Threats (ACTT), which is a multiagency law enforcement partnership in Arizona; and (3) the South Texas Campaign (STC), which integrates CBP resources and facilitates coordination with other homeland security partner agencies. Through these collaborative mechanisms, DHS and CBP have coordinated border security efforts in (1) information sharing, (2) resource targeting and prioritization, and (3) leveraging of assets. Through the ACTT, interagency partners work jointly to target individuals and criminal organizations involved in illegal cross-border activity. The STC leverages assets of CBP components and interagency partners by shifting resources to high-threat regions and conducting joint operations.

DHS and CBP have established performance measures and reporting processes for the JFC and ACTT in Arizona and the STC in South Texas; however, opportunities exist to strengthen these collaborative mechanisms by assessing results across the efforts and establishing written agreements. Each collaborative mechanism reports on its results to DHS or CBP leadership through a variety of means, such as accomplishment reports and after-action reports. However, CBP has not assessed the JFC and STC mechanisms to evaluate results across the mechanisms. JFC and STC components GAO interviewed identified challenges with managing resources and sharing best practices across the mechanisms. For example, officials from all five JFC components GAO interviewed highlighted resource management challenges, such as inefficiencies in staff conducting dual reporting on operations to CBP leadership. Best practices for interagency collaboration call for federal agencies engaged in collaborative efforts to create the means to monitor and evaluate their efforts to enable them to identify areas for improvement. An assessment of the JFC and STC could provide CBP with information to better address challenges the mechanisms have faced. In addition, DHS has not established written agreements with partners in the ACTT and STC Unified Command—the entity within STC used for coordinating activities among federal and state agencies—consistent with best practices for sustaining effective collaboration. Officials from 11 of 12 partner agencies GAO interviewed reported coordination challenges related to the ACTT and STC Unified Command, such as limited resource commitments by participating agencies and lack of common objectives.

GAO recommends that CBP assess the JFC and STC, and that DHS, among other things, establish written agreements with ACTT and the STC Unified Command partners.

Unmanned Aerial Systems: Department of Homeland Security's Review of U.S. Customs and Border Protection's Use and Compliance with Privacy and Civil Liberty Laws and Standards**Number:** [GAO-14-849R](#)**Date:** September 30, 2014

Summary: In its review of the U.S. Customs and Border Protection's (CBP) unmanned aerial systems (UAS) program, the Department of Homeland Security (DHS) reported that CBP has an oversight framework and procedures for its UAS program that help ensure its compliance with privacy and civil liberty laws and standards. DHS's review contains information on CBP procedures on collecting, retaining, storing, and disseminating images from UAS, among others, to help ensure compliance with privacy and civil liberty laws and standards. DHS's review did not address the extent to which CBP had institutionalized these procedures in written policies. However, GAO found that CBP has taken steps to document these procedures and has issued or plans to issue policies to institutionalize the procedures that help protect privacy and civil liberties.

DHS's review found that CBP's use of UAS is not limited to border and coastal areas of the United States. According to DHS's review, the location of UAS operations is limited by Federal Aviation Administration (FAA) requirements and CBP's policies and procedures. DHS's review did not address the extent to which CBP's UAS operations are in border and coastal areas of the United States. GAO analysis of CBP UAS flight hour data found that over 80 percent of UAS flight hours were associated with border and coastal areas of the United States.

DHS OIG Reports**Independent Review of U.S. Coast Guard's Reporting of FY 2013 Drug Control Performance Report****Number:** [OIG-14-35](#)**Date:** February 11, 2014

Summary: KPMG reviewed the Performance Summary Report of the U.S. Department of Homeland Security's (DHS) U.S. Coast Guard (USCG) for the year ended September 30, 2013. USCG's management is responsible for the Performance Summary Report.

Management of USCG prepared the Performance Summary Report to comply with the requirements of the Office of National Drug Control Policy (ONDCP) Circular, *Accounting of Drug Control Funding and Performance Summary*, dated January 18, 2013 (the Circular).

Based on KPMG's review, nothing came to their attention that caused them to believe that the Performance Summary Report for the year ended September 30, 2013, referred to above, is not fairly stated in all material respects, in conformity with the criteria set forth in the Circular.

Review of U.S. Immigration and Customs Enforcement's Reporting of FY 2013 Drug Control Performance Summary Report**Number:** [OIG-14-38](#)**Date:** February 12, 2014

Summary: KPMG reviewed the accompanying Performance Summary Report of the U.S. Department of Homeland Security's (DHS) Immigration and Customs Enforcement (ICE) for the

year ended September 30, 2013. ICE's management is responsible for the Performance Summary Report.

Management of ICE prepared the Performance Summary Report to comply with the requirements of the Office of National Drug Control Policy (ONDCP) Circular, *Accounting of Drug Control and Performance Summary*, dated January 18, 2013 (the Circular).

Based on KPMG's review, nothing came to their attention that caused them to believe that the Performance Summary Report for the year ended September 30, 2013, referred to above, is not fairly stated, in all material respects, in conformity with criteria set forth in the Circular.

Independent Review of U.S. Customs and Border Protection's Reporting of FY 2013 Drug Control Performance Summary Report

Number: [OIG-14-40](#)

Date: February 12, 2014

Summary: KPMG reviewed the accompanying Performance Summary Report of the U.S. Department of Homeland Security's (DHS) Customs and Border Protection (CBP) for the year ended September 30, 2013. CBP's management is responsible for the Performance Summary Report.

Management of CBP prepared the Performance Summary Report to comply with the requirements of the Office of National Drug Control Policy (ONDCP) Circular, *Accounting of Drug Control and Performance Summary*, dated January 18, 2013 (the Circular).

Based on KPMG's review, except as noted below, nothing came to their attention that caused them to believe that the Performance Summary Report for the year ended September 30, 2013, referred to above, is not fairly stated, in all material respects, in conformity with the criteria set forth in the Circular.

The Performance Summary Report for the year ended September 30, 2013, referred to above, does not include a performance measure for the Automation Modernization Drug Control Budget Decision Unit identified in the Detailed Accounting Submission for the year ended September 30, 2013, as required by section 7b(4) of the Circular.

U.S. Customs and Border Protection's Workload Staffing Model

Number: [OIG-14-117](#)

Date: July 24, 2014

Summary: In a statement accompanying the *Department of Homeland Security Appropriations Act, 2012*, Congress directed CBP to report on its allocation for field operations and update the ports of entry staffing model. To improve operations, CBP developed a three-pronged Resource Optimization Strategy. The second prong of the strategy is the Workload Staffing Model, which CBP uses to identify staffing needs for its Office of Field Operations' CBP Officers at ports of entry. We conducted this audit to determine the reliability of the Workload Staffing Model in establishing the number of CBP Officers needed to fulfill mission requirements.

CBP's Workload Staffing Model includes a sound methodology to determine its staffing needs for CBP Officers and identify staffing shortages. However, the results of the model may not be

accurate because CBP cannot ensure that the data entered into the model is reliable. CBP also does not have adequate internal controls over the model. Specifically, CBP's Office of Field Operations does not (1) catalog, track, and validate all data and systems used in workload calculations; (2) systematically approve changes and additions to the Workload Staffing Model; and (3) have written policies and procedures on developing and using the model. In its December 2013 *Strategy and Action Plan (2014-2017)*, CBP acknowledges concerns about data from other systems used in the Workload Staffing Model. CBP has contracted to automate the model, which should address the issues we identified. To ensure that the automated model is accurate, complete, and meets its needs, CBP should conduct an independent verification and validation of the updated model, as well as the data entered into it.

Improving data reliability and strengthening internal controls over the Workload Staffing Model would help CBP ensure that its budget requests accurately reflect CBP Officer staffing needs. It would also help ensure that CBP is allocating staffing resources efficiently. With confidence in the model's reliability and accuracy, Congress will be able to make more informed decisions when considering appropriations for additional CBP officers.

Goal 2.2: Safeguard and Expedite Lawful Trade and Travel

GAO Reports

Maritime Infrastructure: Key Issues Related to Commercial Activity in the U.S. Arctic over the Next Decade

Number: [OIG-14-299](#)

Date: April 18, 2014

Summary: Commercial U.S. Arctic maritime activities are expected to be limited for the next 10 years, according to industry representatives, due to a variety of factors. Interviews with industry representatives highlighted a variety of general challenges related to operating in the Arctic, such as geography, extreme weather, and hard-to-predict ice floes. Industry-specific factors were also cited as contributing to limited commercial activity. For example, shipping companies noted higher costs with Arctic transit; cruise industry groups noted a lack of demand for Arctic cruises from the mainstream cruise-consumer base, and oil companies last drilled offshore exploratory wells in the U.S. Arctic in 2012.

Although the activity will likely be limited, federal, state, and local stakeholders have taken some actions to plan for future maritime-infrastructure investments. Some of these actions address factors that, as identified by industry representatives, contribute to the current and expected limited maritime activity in the U.S. Arctic. For example, the U.S. Army Corps of Engineers (USACE), in collaboration with the State of Alaska, has taken steps to study the development of an Arctic deepwater port; the lack of which is a factor identified by mining representatives as contributing to the expected limited mining activity in the U.S. Arctic. The U.S. Coast Guard (USCG) is in the preliminary phase of seeking to acquire a new polar icebreaker, which could be used for emergency response, research assistance, or patrols. The National Oceanic and Atmospheric Administration (NOAA) and the Alaska government are working to improve mapping, charting, and weather information for the U.S. Arctic.

The Committee on the Marine Transportation System (CMTS) published the U.S. Arctic Marine Transportation System: Overview and Priorities for Action in July 2013, which prioritized actions for developing Arctic maritime infrastructure and identified the lead agency for each action. This report prioritized two broad categories to be addressed in the near term: information infrastructure, such as mapping and charting, and response services, such as search and rescue. Implementation of the report's actions is at the discretion of each federal agency; however, according to CMTS officials, CMTS is currently developing a process to regularly monitor agencies' progress in addressing the recommended actions.

Trusted Travelers: Programs Provide Benefits, but Enrollment Processes Could Be Strengthened

Number: OIG-14-483

Date: May 30, 2014

Summary: As of January 2014, there were about 2.5 million people enrolled in U.S. Customs and Border Protection's (CBP) four trusted traveler programs—which provide expedited travel for preapproved, low-risk travelers and cargo—and enrollments more than quadrupled over the past 5 fiscal years. About 43 percent of trusted travelers were enrolled in Global Entry, operating at select air ports of entry (POE) and about 38 percent were enrolled in NEXUS, operating at northern border POEs. Trusted traveler entries into the United States increased from fiscal years 2009 through 2013. For example, entries through lanes for the Secure Electronic Network for Travelers Rapid Inspection (SENTRI) program, operating at southern border POEs, increased from 5.9 million to 12.6 million vehicles.

CBP has designed and implemented trusted traveler enrollment processes, but could improve key areas to enhance and assess consistency and efficiency in those processes. U.S. citizens and foreign nationals seek to enroll in CBP's trusted traveler programs through an application vetted by CBP and an in-person interview. CBP has taken steps to improve the efficiency of the application-vetting process by, for example, automating background checks. However, CBP has not assessed the feasibility of various other practices for improving efficiency in enrollment processes, such as conducting group briefings for applicants on the programs. As of August 2013, CBP had a backlog of pending applications, as there were about 90,000 applications pending CBP vetting, and another 33,000 applicants who had not scheduled an interview. Assessing the feasibility of various practices, consistent with program management standards, could better position CBP to improve application-processing times. Further, CBP has designed some processes for the trusted traveler applicant interview process to help ensure consistency across enrollment centers; however, GAO identified variations in interviews and application denial rates, indicating that interviews may not be conducted consistently across enrollment centers. For example, GAO observed interviews that did not consistently follow procedures laid out in CBP guidance at 2 of the 3 centers where GAO observed interviews. Establishing a mechanism for CBP officers to document the kinds of questions asked and the nature of the applicants' responses could better position CBP to help ensure that interviews are conducted consistently. In addition, CBP has implemented trusted traveler programs that allow participating low-risk citizens from nine countries to use Global Entry kiosks at select air POEs. CBP has discussed information about other countries' operational procedures for sharing applicant-vetting results, but has not documented this information for seven of the countries, consistent with internal control standards. Without such documentation, there is no institutional

record that those countries' procedures for vetting applicants help to ensure that only low-risk applicants are enrolled.

Trusted travelers generally experience shorter wait times than regular travelers, and CBP spends less time inspecting trusted travelers at POEs than regular travelers. GAO's analysis of CBP data showed that primary inspections took about twice as long or longer on average for regular travelers than for trusted travelers at 11 of 14 SENTRI crossings and 12 of 18 NEXUS crossings in fiscal year 2013. GAO's analysis of CBP data also indicates that trusted travelers commit fewer border violations, such as smuggling, than regular travelers.

DHS OIG Reports

Enhancements in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs

Number: [OIG-14-139](#)

Date: September 10, 2014

Summary: The United States Customs and Border Protection (CBP) employs radio frequency identification technology in its Trusted Traveler Programs to allow pre-screened travelers expedited processing at designated ports of entry. Radio frequency identification is a form of automatic identification and data capture technology that uses radio frequencies to transmit information. The flexibility and portability of radio frequency identification technology has introduced new security risks to agency systems, such as cloning of an identification tag and the security of the database that stores personal data. Without effective security controls and procedures over this technology and its supporting infrastructure, unauthorized individuals could modify identification tag content or access sensitive data stored in the system databases.

Our overall objective was to determine whether CBP has effectively managed the implementation of radio frequency identification technology. In addition, we determined whether the component had implemented effective controls to comply with DHS information security program requirements.

CBP implemented effective physical controls over the readers and computer equipment supporting the trusted traveler systems at the ports of entry visited. Also, CBP implemented effective controls on the servers and database that support the Trusted Traveler Programs. Further, CBP had secured the personal information collected under the component's Trusted Traveler Programs and minimized the risk of using the radio frequency identification technology by restricting information stored on the trusted traveler cards.

However, CBP can make further improvements by implementing the required security settings on the system that supports its Trusted Traveler Programs. Also, administrators that manage the system must receive specialized training annually to ensure that they have the skills necessary to secure the data collected under the Trusted Traveler Programs.

We are making two recommendations to the Assistant Commissioner and Chief Information Officer to improve the security of its systems that support the Trusted Traveler Programs. CBP concurred with all recommendations and has begun to take actions to implement them.

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

No GAO or DHS OIG reports were available that aligned to this goal.

Mission 3: Enforce and Administer Our Immigration Laws

Goal 3.1: Strengthen and Effectively Administer the Immigration System

GAO Reports

Student and Exchange Visitor Program: DHS Needs to Assess Risks and Strengthen Oversight of Foreign Students with Employment Authorization

Number: [GAO-14-356](#)

Date: February 27, 2014

Summary: U.S. Immigration and Customs Enforcement (ICE), a component of the Department of Homeland Security (DHS), has not identified or assessed fraud or noncompliance risks posed by schools that recommend and foreign students approved for optional practical training (OPT), in accordance with DHS risk management guidance. ICE's Student and Exchange Visitor Program (SEVP) officials consider OPT to be a low-risk employment benefit for foreign students because, in part, they believe foreign students approved for OPT do not have an incentive to jeopardize their legal status in the United States. However, SEVP has not determined potential risks in OPT. Further, officials from the Counterterrorism and Criminal Exploitation Unit (CTCEU), ICE's investigative unit, and ICE field agents GAO interviewed have identified potential risks involving OPT based on prior and ongoing investigations. For example, ICE field agents identified cases where school officials recommended OPT for foreign students to work outside of their major areas of study, which is not allowed under ICE regulations.

GAO recommends that ICE, among other things, identify and assess OPT-related risks and require additional employment information from students and schools. DHS concurred with the recommendations.

DHS OIG Reports

U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges

Number: [OIG-14-112](#)

Date: July 23, 2014

Summary: The USCIS Chief Information Officer has established key IT management capabilities to support mission needs, including creating a draft IT strategic plan, developing an enterprise architecture, implementing IT acquisition review and systems engineering life cycle processes, and leading the advancement of agile methodologies for software development. However, additional progress is needed to: 1) Coordinate across internal divisions, 2) ensure that the IT environment fully supports USCIS' mission needs, and 3) ensure staff members know which systems to use and which systems are available to perform their specific job functions.

OIG recommended USCIS CIO: 1) Finalize the IT strategic plan. 2) Develop a plan to address senior level staffing vacancies. 3) Coordinate with system owners to ensure users are provided with adequate training. 4) Develop a plan to refresh outdated IT infrastructure.

Goal 3.2: Prevent Unlawful Immigration

GAO Reports

Additional Actions Could Strengthen DHS Efforts to Address Sexual Abuse

Number: [GAO-14-38](#)

Date: November 20, 2013

Summary: The Department of Homeland Security's (DHS) U.S. Immigration and Customs Enforcement (ICE) sexual abuse and assault allegations data are not complete, a fact that could limit their usefulness for detention management. ICE's data system described 215 allegations of sexual abuse and assault from October 2009 through March 2013 in facilities that had over 1.2 million admissions; however, ICE data did not include all reported allegations. For example, GAO was unable to locate an additional 28 allegations detainees reported to the 10 facilities GAO visited—or 40 percent of 70 total allegations at these 10 facilities—because ICE field office officials did not report them to ICE headquarters. ICE issued guidance on reporting sexual abuse and assault allegations, but has not developed controls to ensure that field office officials responsible for overseeing all facilities are reporting allegations to ICE headquarters.

Detainees may also face barriers to reporting abuse, such as difficulty reaching the DHS Office of Inspector General (OIG) telephone hotline, one of various means for reporting abuse. For example, GAO's review of data maintained by ICE's phone services contractor for fiscal years 2010 through 2012 showed that approximately 14 percent of calls placed to the hotline from about 210 facilities did not go through because, for example, the call was not answered. DHS included various SA-API provisions in three of four sets of detention standards it uses at detention facilities, but does not have reliable and consistent information to determine which provisions apply to which individual facilities.

GAO recommends that DHS (1) develop additional controls to ensure all allegations are reported to headquarters, (2) coordinate OIG access to hotline connectivity data, (3) document and maintain reliable information on detention standards, and (4) develop a process for performing oversight of SA-API provisions consistently across facilities. DHS concurred and reported actions to address the recommendations.

DHS OIG Reports

ICE's Release of Immigration Detainees (Revised)

Number: [OIG-14-116](#)

Date: August 7, 2014

Summary: The OIG determined the execution of the releases was problematic. Insufficient U.S. Immigration and Customs Enforcement (ICE) executive leadership planning and limited

engagement with its Enforcement and Removal Operations field offices contributed to the timing and number of alien releases. Prior to the detainee releases, ICE executive leadership did not communicate effectively with Enforcement and Removal Operations, and did not inform DHS leadership or the Executive Office of the President about the budget shortfall. In addition, ICE did not notify DHS' Secretary about plans to release aliens as a remedy for the budget shortfall.

The OIG made the following recommendations:

- Develop and implement a plan to provide Enforcement and Removal Operations reliable and transparent funding sources to manage detention bed space efficiently and effectively.
- Develop and implement a plan to improve transparency in tracking and reporting ICE budget expenditures to the DHS Chief Financial Officer, the Executive Office of the President, and Congressional Appropriations committees.
- Pursue budget authority to obtain no year or 5-year appropriations to fund detention of arriving aliens.
- Pursue budget authority to obtain funding for the full costs of the detention bed space mandate.

The DHS Visa Security Program

Number: [OIG-14-137](#)

Date: September 10, 2014

Summary: The Department of Homeland Security (DHS) Visa Security Program is intended to prevent terrorists, criminals, and other ineligible applicants from receiving visas. DHS assigns special agents with expertise in immigration law and counterterrorism to U.S. diplomatic posts overseas to perform visa security activities. We reviewed the program's effectiveness in preventing ineligible applicants from receiving U.S. visas; DHS's annual reporting to Congress on the program's expansion; and the efforts to expand the program to additional overseas posts, including the potential impact of a new initiative, the Pre-Adjudicated Threat Recognition and Intelligence Operations Team.

U.S. Immigration and Customs Enforcement (ICE) is required to employ mechanisms that measure and accurately report the program's performance to determine its value. However, current performance measures for the Visa Security Program do not include key aspects to determine its effectiveness. In addition, ICE has not taken actions to assure that (1) data needed to assess program performance is collected and reported, (2) consular officers receive appropriate advice and training, and (3) Visa Security Program hours are tracked and used to determine staffing and funding needs. Without these types of information, ICE cannot ensure that the Visa Security Program is operating as intended.

DHS has consistently delivered their annual reports to Congress late, reducing their usefulness. ICE should take appropriate steps to ensure that Congress receives future reports in a timely manner.

To date, ICE has established only 20 visa security units. Congressional leaders have repeatedly expressed concerns that the program has not expanded to more visa-issuing posts. ICE's responses to these concerns have stressed funding challenges, a limited number of trained special agents, and Department of State challenges to make space and provide support for DHS' overseas presence. According to ICE officials, a solution to the program's slow expansion may be the Pre-Adjudicated Threat Recognition and Intelligence Operations Team. ICE officials explained that this new

initiative will eventually be capable of screening visa applications from all visa-issuing posts. However, because it was still being tested at the time of our review, we were not able to determine its effectiveness.

We are making 10 recommendations to improve the Visa Security Program. ICE concurred with each of the recommendations.

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 Facilities: Selected Facilities' Emergency Plans Generally Reflect Federal Guidance

Number: [GAO-14-101](#)

Date: October 25, 2013

Summary: Federal agencies occupying facilities owned or leased by the General Services Administration (GSA) are responsible for preparing and maintaining occupant emergency plans (OEP), with assistance or guidance from the Federal Protective Service (FPS) and others, and the majority of selected federal facilities' OEPs GAO reviewed reflect federal guidance. As required by federal regulations, all 20 selected facilities had OEPs and had designated officials, who are responsible for maintaining OEPs and initiating action according to the OEP in the event of an emergency, including the evacuation of facility occupants. Consistent with federal guidance, officials at 19 of the 20 selected facilities reported that they review and update OEPs at least annually, and officials at 1 facility said they were in the process of updating their OEP. When requested, FPS provides OEP guidance, such as templates to facility officials. Officials at 14 facilities reported using FPS guidance or feedback for their OEPs, officials at 1 facility reported not using FPS guidance, and officials at 5 facilities said they used their own agency's guidance. FPS also checks OEPs during periodic facility security assessments--conducted at least every 3 to 5 years-- to assess overall facility risk. GSA officials said they have a role in coordinating directly with facilities to provide guidance and feedback on OEPs, and to help facility officials plan drills and exercises. To assist agency officials as they develop OEPs that best fit individual facilities and agency needs, the Interagency Security Committee (ISC), a Department of Homeland Security--chaired policy development organization, in April 2010 identified 10 minimum elements, such as exercises or evacuating occupants with special needs, that should be addressed in an OEP. Thirteen of the 20 selected facilities addressed all 10 minimum elements in OEPs or related documents. Seven facilities' OEPs did not address at least 1 of the 10 elements; however, lack of an element does not necessarily indicate potential vulnerabilities for that facility because the intent of the element may be addressed by other procedures or modified based on facility characteristics. The 20 selected facility OEPs were unique to each facility and how OEPs addressed particular elements.

Officials at 14 of 20 facilities identified evacuation challenges. The most frequently cited challenges included employee apathy toward participating in drills, accounting for employees, and keeping contact information updated. Officials at all but one facility, which was updating its OEP, reported various ways they addressed evacuation challenges, including using technology such as entry scan systems and radios to track and communicate with employees and making evacuation training more interesting to employees. Other incidents and emerging threats also prompted officials to change OEPs or evacuation training. Officials at 6 facilities did not report challenges.

GPS Disruptions: Efforts to Assess to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced**Number:** [GAO-14-15](#)**Date:** November 6, 2013

Summary: To assess the risks and potential effects from disruptions in the Global Positioning System (GPS) on critical infrastructure, the Department of Homeland Security (DHS) published the GPS National Risk Estimate (NRE) in 2012. In doing so, DHS conducted a scenario-based risk assessment for four critical infrastructure sectors using subject matter experts from inside and outside of government. Risk assessments involve complex analysis, and conducting a risk assessment across multiple sectors with many unknowns and little data is challenging. DHS's risk management guidance can be used to help address such challenges. However, we found the NRE lacks key characteristics of risk assessments outlined in DHS's risk management guidance and, as a result, is incomplete and has limited usefulness to inform mitigation planning, priorities, and resource allocation. A plan to collect and assess additional data and subsequent efforts to ensure that the risk assessment is consistent with DHS guidance would contribute to more effective GPS risk management.

A 2004 presidential directive requires the Department of Transportation (DOT), in coordination with DHS, to develop backup capabilities to mitigate GPS disruptions, and the agencies have initiated a variety of efforts that contribute to fulfilling the directive. However, due to resource constraints and other reasons, the agencies have made limited progress in meeting the directive, and many tasks remain incomplete, including identifying GPS backup requirements and determining suitability of backup capabilities. Furthermore, the agencies' efforts have been hampered by a lack of effective collaboration. In particular, DOT and DHS have not clearly defined their respective roles, responsibilities, and authorities or what outcomes would satisfy the presidential directive. Without clearly defining both roles and desired outcomes, DOT and DHS cannot ensure that they will satisfy mutual responsibilities. Implementing key elements of effective collaboration would allow the agencies to address many uncertainties regarding fulfillment of their presidential policy directive.

Selected critical infrastructure sectors employ various strategies to mitigate GPS disruptions. For example, some sectors can rely on timing capabilities from other sources of precise time in the event of GPS signal loss. However, both the NRE and stakeholders we interviewed raised concerns about the sufficiency of the sectors' mitigation strategies. Federal risk management guidance requires DHS to work with federal agencies and critical infrastructure sector partners to measure the nation's ability to reduce risks to critical infrastructure by using a process that includes metrics. We found that DHS has not measured the effectiveness of sector mitigation efforts to GPS disruptions and that, as a result, DHS cannot ensure that the sectors could sustain essential operations during GPS disruptions. The lack of agreed-upon metrics to measure the effectiveness of sector mitigation efforts hinders DHS's ability to objectively assess improvements, track progress, establish accountability, provide feedback mechanisms, or inform decision makers about the appropriateness of the mitigation activities.

DHS should ensure that its GPS risk assessment approach is consistent with DHS guidance; develop a plan to measure the effectiveness of mitigation efforts; and DOT and DHS should improve collaboration.

Critical Infrastructure: Assessment of the Department of Homeland Security's Report on the Results of its Critical Infrastructure Partnership Streamlining Efforts**Number:** [GAO-14-100R](#)**Date:** November 18, 2013

Summary: The Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) was directed by the Senate and House Committees on Appropriations to provide a report on the results of a review to streamline the processes for coordinating and sharing information with its critical infrastructure (CI) protection partners. GAO was unable to assess the extent to which NPPD's streamlining efforts were designed to ensure progress in four areas--mission clarity, useful and actionable work products, efficacy of planning and information sharing, and cost savings--because DHS's response does not discuss NPPD efforts to streamline those processes. Specifically, GAO's analysis of DHS's response showed that DHS provided information on NPPD efforts to coordinate and share information with its public and private partners (e.g., CI owners and operators) and the results of some of those efforts but did not provide information about any NPPD efforts to streamline the processes for coordination and information sharing. For example, DHS's response includes a section on coordinating and executing plans--one of the five topic areas that NPPD was required to include in its report--that describes who NPPD's partners are and ways that NPPD coordinates and executes plans with these various stakeholders. In addition, the response describes steps NPPD plans to take that are intended to improve the coordination and execution of plans. However, the response did not describe steps NPPD has taken or plans to take, if any, to streamline efforts associated with the coordination and execution of plans or how, if at all, coordination and information sharing might be affected. NPPD officials stated that they agreed with the above and that they are currently working to provide the committees with information on their streamlining efforts.

Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology**Number:** [GAO-14-125](#)**Date:** January 28, 2013

Summary: The five identified federal agencies (Departments of Homeland Security, Commerce, Justice, and Transportation and Federal Communications Commission (FCC)) have to varying degrees, coordinated cybersecurity-related activities with state and local governments. These activities included (1) supporting critical infrastructure protection-related planning, (2) issuing grants, (3) sharing information, (4) providing technical assistance, and (5) regulating and overseeing essential functions. However, except for supporting critical infrastructure planning, federal coordination of these activities was generally not targeted towards or focused on the cybersecurity of state and local public safety entities involved in handling 911 emergency calls.

Under the critical infrastructure protection planning activity, the Department of Homeland Security (DHS) coordinated with state and local governments and other federal stakeholders to complete the Emergency Services Sector-Specific Plan. The plan is to guide the sector, including the public safety entities, in setting protective program goals and objectives, identifying assets, assessing risks, prioritizing infrastructure components and programs to enhance risk mitigation, implementing protective programs, measuring program effectiveness, and incorporating research and development of technology initiatives into sector planning efforts. It also addressed aspects of cybersecurity of the current environment. However, the plan did not address the development and implementation of more interconnected, Internet-based planned information technologies, such as the next

generation of 911 services. According to DHS officials, the plan did not address these technologies, in part, because the process for updating the sector-specific plan will begin after the release of the revised National Infrastructure Protection Plan--a unifying framework to enhance the safety of the nation's critical infrastructure. A revised plan was released in December 2013, and, according to DHS, a new sector-specific plan is estimated to be completed in December 2014. Until DHS, in collaboration with stakeholders, addresses the cybersecurity implications of the emerging technologies in planning activities, information systems are at an increased risk of failure or being unavailable at critical moments.

Under the other four activities, federal agencies performed some coordination related activities for public safety entities including administering grants for information technology enhancements, sharing information about cyber-based attacks, and providing technical assistance through education and awareness efforts.

GAO recommends that the Secretary of Homeland Security collaborate with emergency services sector stakeholders to address the cybersecurity implications of implementing technology initiatives in related plans.

Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Approach

Number: [GAO-14-464T](#) (Testimony)

Date: March 26, 2014

Summary: GAO's prior work has identified several key factors that are important for the Department of Homeland Security (DHS) to implement its partnership approach with industry to protect critical infrastructure. DHS has made some progress in implementing its partnership approach, but has also experienced challenges coordinating with industry partners that own most of the critical infrastructure.

- **Recognizing and Addressing Barriers to Sharing Information.** Since 2003, GAO has identified information sharing as key to developing effective partnerships. In July 2010, GAO reported some barriers affecting the extent to which cyber-related security information was being shared between federal and industry partners. GAO recommended that DHS work with industry to focus its information-sharing efforts. DHS concurred and has taken some steps to address the recommendation, including sponsoring clearances for industry.
- **Sharing Results of DHS Assessments with Industry.** GAO has found that DHS security assessments can provide valuable insights into the strengths and weaknesses of critical assets and drive industry decisions about investments to enhance security. In a May 2012 report, GAO found that DHS was sharing the results of its assessments with industry partners, but these results were often late, which could undermine the relationship DHS was attempting to develop with these partners. GAO recommended that DHS develop time frames and milestones to ensure the timely delivery of the assessments to industry partners. DHS concurred and reported that it has efforts underway to speed the delivery of its assessments.
- **Measuring and Evaluating Performance of DHS Partnerships.** GAO's prior work found that taking a systematic approach to gathering feedback from industry owners and operators and measuring the results of these efforts could help focus greater attention on targeting potential problems and areas needing improvement. In an April 2013 report, GAO

examined DHS's chemical security program and assessed, among other things, the extent to which DHS has communicated and worked with industry owners and operators to improve security. GAO reported that DHS had increased its efforts to communicate and work with industry to help them enhance security at their facilities. However, GAO found that DHS was not obtaining systematic feedback on its outreach. GAO recommended that DHS explore opportunities and take action to systematically solicit and document feedback on industry outreach. DHS concurred and reported that it had taken action to address the recommendation.

However, the cyber security of infrastructure remains on GAO's high-risk list and more needs to be done to accelerate the progress made. DHS still needs to fully implement the many recommendations on its partnership approach (and other issues) made by GAO and inspectors general to address cyber challenges.

Federal Facility Security: Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards

Number: [GAO-14-86](#)

Date: April 7, 2014

Summary: Three of the nine selected agencies' risk assessment methodologies that GAO reviewed—the Department of Energy (DOE), the Department of Justice (DOJ), and the Department of State (State)—fully align with the Interagency Security Committee's (ISC) risk assessment standards, but six do not—the Department of the Interior (DOI), the Department of Veterans Affairs (VA), the Federal Protective Service (FPS), the Federal Emergency Management Agency (FEMA), the Nuclear Regulatory Commission (NRC), and the Office of Personnel Management (OPM). As a result, these six agencies may not have a complete understanding of the risks facing approximately 52,000 federal facilities and may be less able to allocate security resources cost-effectively at the individual facility level or across the agencies' facility portfolios. ISC's *The Risk Management Process for Federal Facilities (RMP)* standard requires that agencies' facility risk assessment methodologies must (1) consider all of the undesirable events identified in the *RMP* as possible risks to federal facilities, and (2) assess the threat, consequences, and vulnerability to specific undesirable events. Six of the nine agencies' methodologies GAO reviewed do not align with ISC's standards because the methodologies do not (1) consider all of the undesirable events in the *RMP* or (2) assess threat, consequences, or vulnerability to specific undesirable events. For example, five agencies (DOI, VA, FEMA, FPS, and NRC), do not assess the threat, consequences, or vulnerability to specific undesirable events, as ISC requires. The reasons why varied; for example, VA said that its methodology was in place before ISC issued its standards. Officials from that agency told us they were working to update their methodology.

ISC has issued a series of physical security standards and guidance to assist member agencies with developing their risk assessment methodologies, but does not know the extent to which its 53 member agencies comply with its standards, including its risk assessment standards, because it does not monitor agencies' compliance. ISC does not monitor compliance or have an approach to do so that incorporates outreach to agencies regarding their compliance status. Officials stated that they would like to monitor agencies' compliance, but limited resources and other priorities, such as developing standards and guidance, have prevented them from doing so. However, ISC has the authority to create a working group from its member agencies to help it perform its duties. In the absence of ISC's monitoring, agencies' risk assessment methodologies may not align with ISC's

standards. In addition, although ISC issued risk assessment guidance in August 2013, this guidance is limited. For example, the guidance does not describe how to incorporate threat, consequence, or vulnerability assessments of specific undesirable events into a risk assessment methodology. Not having appropriate guidance is inconsistent with federal internal-control standards designed to promote effectiveness and efficiency.

Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity

Number: [GAO-14-459](#)

Date: June 5, 2014

Summary: Actions taken by the Department of Homeland Security (DHS) and two of its component agencies, the U.S. Coast Guard and Federal Emergency Management Agency (FEMA), as well as other federal agencies, to address cybersecurity in the maritime port environment have been limited.

- While the Coast Guard initiated a number of activities and coordinating strategies to improve physical security in specific ports, it has not conducted a risk assessment that fully addresses cyber-related threats, vulnerabilities, and consequences. Coast Guard officials stated that they intend to conduct such an assessment in the future, but did not provide details to show how it would address cybersecurity. Until the Coast Guard completes a thorough assessment of cyber risks in the maritime environment, the ability of stakeholders to appropriately plan and allocate resources to protect ports and other maritime facilities will be limited.
- Maritime security plans required by law and regulation generally did not identify or address potential cyber-related threats or vulnerabilities. This was because the guidance issued by Coast Guard for developing these plans did not require cyber elements to be addressed. Officials stated that guidance for the next set of updated plans, due for update in 2014, will include cybersecurity requirements. However, in the absence of a comprehensive risk assessment, the revised guidance may not adequately address cyber-related risks to the maritime environment.
- The degree to which information-sharing mechanisms (e.g., councils) were active and shared cybersecurity-related information varied. Specifically, the Coast Guard established a government coordinating council to share information among government entities, but it is unclear to what extent this body has shared information related to cybersecurity. In addition, a sector coordinating council for sharing information among nonfederal stakeholders is no longer active, and the Coast Guard has not convinced stakeholders to reestablish it. Until the Coast Guard improves these mechanisms, maritime stakeholders in different locations are at greater risk of not being aware of, and thus not mitigating, cyber-based threats.
- Under a program to provide security-related grants to ports, FEMA identified enhancing cybersecurity capabilities as a funding priority for the first time in fiscal year 2013 and has provided guidance for cybersecurity-related proposals. However, the agency has not consulted cybersecurity-related subject matter experts to inform the multi-level review of cyber-related proposals—partly because FEMA has downsized the expert panel that reviews grants. Also, because the Coast Guard has not assessed cyber-related risks in the maritime risk assessment, grant applicants and FEMA have not been able to use this information to

inform funding proposals and decisions. As a result, FEMA is limited in its ability to ensure that the program is effectively addressing cyber-related risks in the maritime environment.

GAO recommends that DHS direct the Coast Guard to (1) assess cyber-related risks, (2) use this assessment to inform maritime security guidance, and (3) determine whether the sector coordinating council should be reestablished. DHS should also direct FEMA to (1) develop procedures to consult DHS cybersecurity experts for assistance in reviewing grant proposals and (2) use the results of the cyber-risk assessment to inform its grant guidance.

Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts

Number: [GAO-14-507](#)

Date: September 15, 2014

Summary: During fiscal years 2011 to 2013, various Department of Homeland Security (DHS) offices and components conducted or required thousands of vulnerability assessments of critical infrastructure (CI), but DHS is not positioned to integrate them in order to identify priorities. Although the Homeland Security Act of 2002 and the National Infrastructure Protection Plan (NIPP) call for DHS to integrate CI vulnerability assessments to identify priorities, the department cannot do so because of variation in the areas to be assessed for vulnerability included in the various tools and methods used by DHS. GAO analysis of 10 of these assessment tools and methods found that they consistently included some areas, such as perimeter security, but other areas, such as cybersecurity, were not consistently included in the 10 tools and methods. Also, GAO's analysis and discussions with DHS officials showed that DHS's assessments vary in their length and detail of information collected, and DHS has not established guidance on what areas should be included in a vulnerability assessment, such as vulnerabilities to all-hazards as called for in the NIPP. DHS's Office of Infrastructure Protection (IP) has recognized the challenge of having different approaches and has begun to take action to harmonize them. However, of the 10 assessment tools and methods GAO analyzed, IP's harmonization effort includes two voluntary IP assessment tools and none of the other 8 tools and methods GAO analyzed that are used by other DHS offices and components. By reviewing the tools and methods to identify the areas of vulnerability and level of detail that DHS considers necessary, and establishing guidance for DHS offices and components regarding which areas to include in their assessments, DHS would be better positioned to integrate assessments to enable comparisons and determine priorities between and across CI sectors.

DHS offices and components have not consistently captured and maintained data on vulnerability assessment activities in a way that allows DHS to identify potential duplication or overlap in coverage among vulnerability assessment activities they have conducted or required. As a result, DHS is not positioned to track its activities to determine whether its assessment efforts are potentially duplicative or leave gaps among the CI assessed and thereby better ensure effective risk management across the spectrum of assets and systems, as called for by the NIPP. Developing an approach to collect data consistently would facilitate DHS's identification of potential duplication or overlap in CI coverage. Having consistent data would also better position DHS to minimize the fatigue CI owners expressed experiencing from participation in multiple assessments.

DHS is not positioned to manage an integrated and coordinated government-wide approach for assessments as called for in the NIPP because it does not have sufficient information about the assessment tools and methods conducted or offered by federal entities external to DHS with CI

responsibilities, such as the Environmental Protection Agency, which oversees critical infrastructure activities related to water and wastewater systems. Consequently, opportunities exist for DHS to work with other federal entities to develop guidance as necessary to ensure consistency. Doing so would better position DHS and other federal entities with CI responsibilities to promote an integrated and coordinated approach for conducting vulnerability assessments of CI, as called for in the Homeland Security Act of 2002, presidential directives, and the NIPP.

GAO recommends that DHS identify the areas assessed for vulnerability most important for integrating and comparing results, establish guidance for DHS offices and components to incorporate these areas into their assessments, ensure that assessment data are consistently collected, and work with other federal entities to develop guidance for what areas to include in vulnerability assessments, among other things.

Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise

DHS OIG Reports

Implementation Status of EINSTEIN 3 Accelerated

Number: [OIG-14-52](#)

Date: March 24, 2014

Summary: We audited the National Protection and Programs Directorate's (NPPD) National Cybersecurity Protection System (EINSTEIN 3 Accelerated) that provides an intrusion prevention capability for the Federal Government. Our objectives were to determine its implementation status and whether security and privacy concerns are being addressed to protect the sensitive data processed by the system.

In 2008, NPPD began to deploy the National Cybersecurity Protection System to protect Federal networks and prevent known or suspected cyber threats. NPPD is responsible for the Department's national, non-law enforcement cybersecurity missions. In April 2012, NPPD changed the overall implementation strategy for EINSTEIN 3 Accelerated by procuring commercially-available network defense services. NPPD has begun to deploy EINSTEIN 3 Accelerated to protect Federal networks and expects to reach its full operating capability by the end of fiscal year 2015. In addition, NPPD created its Top Secret Mission Operating Environment, which is a classified network used for EINSTEIN 3 Accelerated analysis. Further, NPPD is finalizing contract negotiations with five Internet service providers to deploy intrusion prevention on 87 percent of Federal agency network traffic. As of September 2013, NPPD established Memorandums of Agreement with 23 Federal agency participants and brought initial protection services to 4 of them. NPPD completed a Privacy Impact Assessment to provide an analysis on how the personally identifiable information collected under EINSTEIN 3 Accelerated will be handled.

Based on our review, we determined that NPPD needs to strengthen the monitoring of the program's implementation and improve the component's ability to handle personally identifiable information as the program matures. Specifically, NPPD must develop implementation measures and a delivery timeline to guide the deployment of intrusion prevention services to its customers on

schedule. Further, NPPD must update its training program and standard operating procedure for minimizing personally identifiable information to ensure analysts understand their roles and responsibilities for handling sensitive information. Finally, NPPD must address minor security vulnerabilities identified in its classified operational environment to further reduce risk to sensitive information.

We are making four recommendations to NPPD to help ensure the implementation of EINSTEIN 3 Accelerated proceeds as scheduled and personally identifiable information processed by the system is protected.

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

GAO Reports

Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent

Number: [GAO-14-34](#)

Date: January 8, 2014

Summary: The eight federal agencies GAO reviewed generally developed, but inconsistently implemented, policies and procedures for responding to a data breach involving personally identifiable information (PII) that addressed key practices specified by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology. The agencies reviewed generally addressed key management and operational practices in their policies and procedures, although three agencies had not fully addressed all key practices. In addition, the implementation of key operational practices was inconsistent across the agencies. The Army, VA, and the Federal Deposit Insurance Corporation had not documented how risk levels had been determined and the Army had not offered credit monitoring consistently. Further, none of the agencies we reviewed consistently documented the evaluation of incidents and resulting lessons learned. Incomplete guidance from OMB contributed to this inconsistent implementation. As a result, these agencies may not be taking corrective actions consistently to limit the risk to individuals from PII-related data breach incidents.

According to agency officials, the Department of Homeland Security's (DHS) role of collecting information and providing assistance on PII breaches, as currently defined by federal law and policy, has provided few benefits. OMB's guidance to agencies requires them to report each PII-related breach to DHS's U.S. Computer Emergency Readiness Team (US-CERT) within 1 hour of discovery. However, complete information from most incidents can take days or months to compile; therefore preparing a meaningful report within 1 hour can be infeasible. US-CERT officials stated they can generally do little with the information typically available within 1 hour and that receiving the information at a later time would be just as useful. Likewise, US-CERT officials said they have little use for case-by-case reports of certain kinds of data breaches, such as those involving paper-based PII, because they considered such incidents to pose very limited risk. Also, the agencies GAO reviewed have not asked for assistance in responding to PII-related incidents from US-CERT, which has expertise focusing more on cyber-related topics. As a result, these

agencies may be expending resources to meet reporting requirements that provide little value and divert time and attention from responding to breaches.

GAO is making 23 recommendations to OMB to update its guidance on federal agencies' response to a data breach and to specific agencies to improve their response to data breaches involving PII. In response to OMB and agency comments on a draft of the report, GAO clarified or deleted three draft recommendations but retained the rest, as discussed in the report.

Information Security: Agencies Need to Improve Cyber Incident Response Practices

Number: [GAO-14-354](#)

Date: May 30, 2013

Summary: Twenty-four major federal agencies did not consistently demonstrate that they are effectively responding to cyber incidents (a security breach of a computerized system and information). Based on a statistical sample of cyber incidents reported in fiscal year 2012, GAO projects that these agencies did not completely document actions taken in response to detected incidents in about 65 percent of cases (with 95 percent confidence that the estimate falls between 58 and 72 percent). For example, agencies identified the scope of an incident in the majority of cases, but frequently did not demonstrate that they had determined the impact of an incident. In addition, agencies did not consistently demonstrate how they had handled other key activities, such as whether preventive actions to prevent the reoccurrence of an incident were taken. Although all 6 selected agencies that GAO reviewed in depth had developed parts of policies, plans, and procedures to guide their incident response activities, their efforts were not comprehensive or fully consistent with federal requirements. In addition, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) conduct CyberStat reviews, which are intended to help federal agencies improve their information security posture, but the reviews have not addressed agencies' cyber incident response practices. Without complete policies, plans, and procedures, along with appropriate oversight of response activities, agencies face reduced assurance that they can effectively respond to cyber incidents.

DHS and a component, the United States Computer Emergency Readiness Team (US-CERT), offer services that assist agencies in preparing to handle cyber incidents, maintain awareness of the current threat environment, and deal with ongoing incidents. Officials from the 24 agencies GAO surveyed said that they were generally satisfied with the assistance provided, and made suggestions to make the services more useful, such as improving reporting requirements. Although US-CERT receives feedback from agencies to improve its services, it has not yet developed performance measures for evaluating the effectiveness of the assistance it provides to agencies. Without results-oriented performance measures, US-CERT will face challenges in ensuring it is effectively assisting federal agencies with preparing for and responding to cyber incidents.

GAO is making recommendations to OMB and DHS to address incident response practices government-wide, particularly in CyberStat meetings with agencies; to the heads of six agencies to strengthen their incident response policies, plans, and procedures; and to DHS to establish measures of effectiveness for the assistance US-CERT provides to agencies.

DHS OIG Reports

DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers

Number: [OIG-14-02](#)

Date: October 25, 2013

Summary: We audited the National Protection and Programs Directorate's (NPPD) efforts in coordinating with cyber operations centers across the Federal Government. The recent increase in cyber attacks has triggered an expansion of security initiatives and collaboration between the Government and the private sector. The National Cybersecurity and Communications Integration Center, which is the operational arm of the Office of Cybersecurity and Communications within NPPD, is responsible for integrating cyber threat information from the five Federal cybersecurity centers and collaborating with these centers in responding to cyber security incidents that may pose a threat to the Nation.

NPPD has taken actions to coordinate and share vital cyber threat information with the five Federal cyber operations centers. In addition, NPPD has increased interagency collaboration and communication through the use of liaisons and participating in regular meetings. Finally, NPPD has issued—in collaboration with the Federal Bureau of Investigation—Joint Indicator Bulletins to assist private sector partners in preventing cyber attacks and protecting intellectual property, trade secrets, and sensitive business information from exploitation and theft.

Still, the Department of Homeland Security (DHS) faces challenges in sharing cyber information among the Federal cyber operations centers. Specifically, DHS must procure cyber tools and technologies to improve its situational awareness efforts. In addition, it needs to work with its cyber operations center partners to develop a standard set of cyber incident reporting categories. Further, DHS has to address insufficient staffing levels that hinder its ability to provide continuous coverage in all mission areas in the National Cyber security and Communications Integration Center operations center and conduct additional technical training needed to improve staff's incident response skills. Finally, it must update the NPPD Continuity of Operations Plan, and finalize and integrate it with the Office of Cybersecurity and Communications' Continuity of Operations Plan and the National Cybersecurity and Communications Integration Center's Continuity of Operations Plan.

We are making seven recommendations to DHS to improve its coordination and collaboration with the Federal cyber operations centers across the Government.

Implementation Status of the Enhanced Cybersecurity Services Program

Number: [OIG-14-119](#)

Date: July 29, 2014

Summary: In February 2013, in an effort to strengthen the Nation's critical infrastructure, the President directed the Department of Homeland Security (DHS), in collaboration with the Secretary of Defense, to expand the Enhanced Cybersecurity Services program to all 16 critical infrastructure sectors. The Enhanced Cybersecurity Services program is a voluntary information sharing initiative in which DHS shares both unclassified and classified indicators of malicious cyber activity with critical infrastructure sector participants.

The National Protection Programs Directorate (NPPD) is primarily responsible for fulfilling the DHS national, non-law enforcement cybersecurity missions. Within NPPD, the Office of Cybersecurity and Communications is responsible for the implementation of the Enhanced Cybersecurity Services program. Our overall objective was to determine the effectiveness of the Enhanced Cybersecurity Services program to disseminate cyber threat and technical information with the critical infrastructure sectors through commercial service providers.

NPPD has made progress in expanding the Enhanced Cybersecurity Services program. For example, as of May 2014, 40 critical infrastructure entities participate in the program. Additionally, 22 companies have signed memorandums of agreement to join the program. Further, NPPD has established the procedures and guidance required to carry out key tasks and operational aspects of the program, including an in-depth security validation and accreditation process. NPPD has also addressed the privacy risk associated with the program by developing a Privacy Impact Assessment. Finally, NPPD has engaged sector-specific agencies and government furnished information providers to expand the program, and has developed program reporting and metric capabilities to monitor the program.

Although NPPD has made progress, the Enhanced Cybersecurity Services program has been slow to expand because of limited outreach and resources. In addition, cyber threat information sharing relies on NPPD's manual reviews and analysis, which has led to inconsistent cyber threat indicator quality.

We are making three recommendations to NPPD to help expand the implementation of the Enhanced Cybersecurity Services program.

Goal 4.4: Strengthen the Cyber Ecosystem

No GAO of DHS OIG reports were available that aligned to this goal.

Mission 5: Strengthen National Preparedness and Resilience

Goal 5.1: Enhance National Preparedness

GAO Reports

National Preparedness: Actions Taken by FEMA to Implement Select Provisions of the Post-Katrina Emergency Management Reform Act of 2006

Number: [GAO-14-99R](#)

Date: November 26, 2013

Summary: In summary, GAO found that the Federal Emergency Management Agency (FEMA) reported taking various actions to address each of the five provisions of the Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act) that GAO reviewed.

- **6 U.S.C. 319 (b)(2)(C):** In response to this provision--which requires FEMA to revise the Catastrophic Incident Annex (the Annex) to the National Response Plan (NRP), now called the National Response Framework (NRF), and finalize and release the Catastrophic Incident Supplement (the Supplement) to the NRP--FEMA revised the Annex, and finalized and released the Supplement, but has not revised the Supplement to reflect the NRF.
- **6 U.S.C. 748 (b):** In response to this provision--which requires FEMA to carry out a national exercise program and conduct periodic national exercises, not less than biennially--FEMA developed the National Exercise Program (NEP) in coordination with other federal agencies and two national councils within the time frame required by the act, and conducted five national exercises since fiscal year 2007.
- **6 U.S.C. 751 (b) and (d):** In response to this provision--which requires FEMA to develop an inventory of federal response capabilities as well as a database for the inventory--FEMA officials said that, taken together, the draft Federal Interagency Operational Plan for the NRF (Response FIOP) and FEMA's Pre-Scripted Mission Assignment (PSMA) Catalogue address the requirement.
- **6 U.S.C. 752 (b):** In response to this provision--which requires FEMA to annually submit to Congress a Catastrophic Resource Report (CRR) that includes estimates of the resources of FEMA and other federal agencies needed for and devoted specifically to developing capabilities at all levels of government necessary to respond to a catastrophic incident--FEMA did not issue CRRs from fiscal year 2007 through fiscal year 2011, issued the first CRR in August 2012, and as of September 2013 FEMA officials said that they intend to issue the second annual CRR by the end of calendar year 2013.
- **6 U.S.C. 753 (c) and (d):** In response to this provision--which requires FEMA's development of pre-scripted mission assignments (PSMA) and presidential certification that federal agencies with responsibilities under the NRP (now NRF) have, among other things, needed operational capabilities to meet the National Preparedness Goal--FEMA issued a PSMA Catalogue, and FEMA officials said that various recently issued and to-be-issued reports and a draft plan should collectively be considered to meet the presidential certification requirement.

Federal Emergency Management Agency: Opportunities to Achieve Efficiencies and Strengthen Operations**Number:** [GAO-14-687T](#) (Testimony)**Date:** July 24, 2014

Summary: GAO's recent and ongoing work examining the Federal Emergency Management Agency's (FEMA) administrative costs of providing disaster assistance highlights opportunities to increase efficiencies and potentially reduce these costs. In September 2012, GAO reported that FEMA's administrative costs for disaster assistance had doubled in size as a percentage of the overall cost of the disasters since fiscal year 1989, and often surpassed its targets for controlling administrative costs. GAO also concluded that FEMA's administrative costs were increasing for all sizes of disasters and for all types of disaster assistance. FEMA issued guidelines intended to improve the efficiency of its efforts and to help reduce administrative costs. However, FEMA did not make this guidance mandatory because it wanted to allow for flexibility in responding to a variety of disaster situations. In 2012, GAO recommended that the FEMA Administrator implement goals for administrative cost percentages and monitor performance to achieve these goals. However, as of June 2014, FEMA had not taken steps to implement GAO's recommendation. GAO's ongoing work indicates that FEMA is implementing a new system to, among other things, collect and analyze data on the administrative costs associated with managing disasters to enable managers to better assess performance. However, according to officials, FEMA is still working on systematically collecting the data. As a result, it is too early to assess whether this effort will improve efficiencies or reduce administrative costs.

GAO has also reported on opportunities to strengthen and increase the effectiveness of FEMA's workforce management. Specifically, GAO reviewed FEMA human capital management efforts in 2012 and 2013 and has made a number of related recommendations, many of which FEMA has implemented; some of which are still underway. For example, GAO recommended that FEMA identify long-term quantifiable mission-critical goals and establish a time frame for completing the development of quantifiable performance measures for workforce planning and training, establish lines of authority for agency-wide efforts related to workforce planning and training, and develop systematic processes to collect and analyze workforce and training data. FEMA concurred and is still working to address these recommendations. For example, FEMA's deployment of its disaster assistance workforce during the response to Hurricane Sandy revealed a number of challenges. In response, according to agency officials, FEMA is, among other things, analyzing its disaster assistance workforce structure to ensure the agency is capable of responding to large and complex incidents. GAO will continue to evaluate these efforts to assess their effectiveness.

In March 2011, GAO reported that FEMA could enhance the coordination of application reviews of grant projects across four of the largest preparedness grants (Urban Areas Security Initiative, State Homeland Security Program, Port Security Grant Program, and Transit Security Grant Program) which have similar goals, fund similar types of projects, and are awarded in many of the same urban areas. GAO recommended that FEMA coordinate the grant application process to reduce the potential for duplication. FEMA has attempted to use data to coordinate two programs and also proposed to consolidate its preparedness grant programs, but FEMA's data system has been delayed, and Congress did not approve FEMA's consolidation proposal for either fiscal year 2013 or 2014.

DHS OIG Reports

Annual Report to Congress on States' and Urban Areas' Management of Homeland Security Grant Programs Fiscal Year 2013

Number: [OIG-14-22](#)

Date: December 20, 2013

Summary: Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007, requires the Department of Homeland Security (DHS), Office of Inspector General (OIG), to audit individual States' management of State Homeland Security Program and Urban Areas Security Initiative grants, and annually submit to Congress a report summarizing the results of those audits. This report responds to the annual reporting requirement and summarizes audits of 10 States and 1 urban area completed in fiscal year 2013: Connecticut, Indiana, Kentucky, Massachusetts, Mississippi, Nebraska, North Carolina, Rhode Island, Virginia, Wisconsin, and Illinois (Urban Areas Security Initiative only).

The objectives of the State and urban area audits were to determine whether each State and urban area distributed and spent the grant funds (1) effectively and efficiently, and (2) in compliance with applicable Federal laws and regulations. We also addressed the extent to which grant funds enhanced the States' and urban area's ability to prevent, prepare for, protect against, and respond to natural disasters, acts of terrorism, and other manmade disasters. The audits included more than \$668 million in State Homeland Security Program and Urban Areas Security Initiative grants awarded to the 10 States and 1 urban area during 3-year or 4-year periods between fiscal years 2006 and 2011.

In most instances, the States and urban area did an efficient and effective job of administering the grant program requirements in compliance with grant guidance and regulations. Additionally, we identified two innovative practices that can be considered for use by other jurisdictions.

Two major areas were identified for improvement: strategic planning and oversight of grant activities. We also identified more than \$5.7 million in questioned costs. We made 76 recommendations addressing these areas.

FEMA Could Realize Millions in Savings by Strengthening Policies and Internal Controls Over Grant Funding for Permanently Relocated Damaged Facilities

Number: [OIG-14-91-D](#)

Date: May 6, 2014

Summary: The objective of the audit was to determine the efficiency and effectiveness of FEMA policies and procedures concerning disaster grant costs associated with permanently relocated facilities. Specifically, we determined whether (1) FEMA's present policies and procedures effectively address how FEMA should use program income to offset permanently relocated facility costs; and (2) internal controls were in place to identify when applicants receive program income to offset permanently relocated facility costs.

The audit included a review of costs for permanently relocated damaged facilities in Mississippi and Louisiana for Hurricane Katrina and in Texas for Hurricane Ike. FEMA could realize millions of dollars in cost savings by strengthening its policies, procedures, and internal controls over Public Assistance grant funding provided for permanently relocated damaged facilities. Specifically, our

audit determined that FEMA's present policies and procedures do not effectively address how FEMA should use program income to offset permanently relocated facility costs. For example, such a revised policy could have saved an estimated \$17.8 million in project costs for the 30 projects that we reviewed in Mississippi. Also, internal controls were not in place to determine when applicants received program income to offset permanently relocated facility costs. Therefore, FEMA should strengthen its policies, procedures, and internal controls over permanently relocated facilities to (1) use program income effectively to offset permanently relocated facility costs and (2) determine when program income is incurred to offset permanently relocated facility costs.

Our two recommendations call for FEMA to initiate improvements that, when implemented, should help strengthen program management, internal controls, and oversight of Public Assistance funding provided for permanently relocated facilities.

FY 2013 FEMA Public Assistance and Hazard Mitigation Grant and Subgrant Audits

Number: [OIG-14-102-D](#)

Date: June 10, 2014

Summary: Of the 59 grant audit reports we issued in FY 2013, 54 reports contained 261 recommendations resulting in potential monetary benefits of \$307.8 million. This amount included \$266.2 million in questioned costs we recommended FEMA disallow because the costs were ineligible or unsupported, and \$41.6 million in unused funds we recommended FEMA deobligate and put to better use. The \$307.8 million in potential monetary benefits represents 24 percent of the \$1.28 billion we audited.

As stated in our four previous capping reports, we continue to find problems with grant management and accounting, ineligible and unsupported costs, and noncompliance with Federal contracting requirements. A significant issue this year was insufficient insurance required to protect grant recipients from future losses. We also noted a sharp increase in questioned costs for ineligible contracting procedures.

Grantees and subgrantees did not always properly account for and expend FEMA PA program and HMGP funds. Federal regulations for grant administration require states, as grantees, to oversee subgrant activities and ensure that subgrantees are aware of and follow Federal regulations designed to ensure financially assisted activities comply with applicable laws and regulations. Many of our findings and reportable conditions indicate that states should do a better job of educating subgrantees and enforcing Federal regulations.

It is FEMA's responsibility to hold states accountable for proper grant administration, especially with regard to contracting practices. We questioned \$108 million more in contract costs in FY 2013 than in FY 2012, mostly because grantees are not ensuring that subgrantees are aware of requirements for complying with Federal procurement regulations.

DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures

Number: [OIG-14-129](#)

Date: August 26, 2014

Summary: The Department of Homeland Security (DHS) supports efforts to develop and execute pandemic contingency plans and preparedness actions as part of the United States Government's

pandemic preparedness strategy. A severe influenza pandemic presents a tremendous challenge, which may affect millions of Americans, cause significant illnesses and fatalities, and substantially disrupt our economic and social stability. It is DHS' responsibility to ensure it is adequately prepared to continue critical operations in the event of a pandemic.

In 2006, Congress appropriated \$47 million in supplemental funding to DHS for necessary expenses to plan, train, and prepare for a potential pandemic. DHS reported that it spent this funding on personal protective equipment, pandemic research, exercises, and medical countermeasures. The Department and components purchased personal protective equipment and medical countermeasures (specifically, antiviral medical countermeasures) to reduce potential effects of a pandemic and ensure the workforce can continue operations. We conducted an audit of the DHS pandemic preparedness efforts to determine if DHS effectively manages its pandemic preparedness supply of personal protective equipment and antiviral medical countermeasures.

DHS did not adequately conduct a needs assessment prior to purchasing pandemic preparedness supplies and then did not effectively manage its stockpile of pandemic personal protective equipment and antiviral medical countermeasures. Specifically, it did not have clear and documented methodologies to determine the types and quantities of personal protective equipment and antiviral medical countermeasures it purchased for workforce protection. The Department also did not develop and implement stockpile replenishment plans, sufficient inventory controls to monitor stockpiles, adequate contract oversight processes, or ensure compliance with Department guidelines. As a result, the Department has no assurance it has sufficient personal protective equipment and antiviral medical countermeasures for a pandemic response. In addition, we identified concerns related to the oversight of antibiotic medical countermeasures.

We made 11 recommendations that when implemented should improve the efficiency and effectiveness of the Department's pandemic preparations.

Goal 5.2: Mitigate Hazards and Vulnerabilities

DHS OIG Reports

FEMA's Dissemination of Procurement Advice Early in Disaster Response Periods

Number: [OIG-14-46-D](#)

Date: February 28, 2014

Summary: Over 8 years since Hurricane Katrina, FEMA has not obligated approximately \$812 million of the \$2.16 billion in authorized mitigation funds. While conducting our audit, FEMA made progress in approving projects and, as of March 2014, FEMA reduced the unobligated amount from \$1.1 billion in September 2012 to \$812 million. This \$812 million represents missed or delayed opportunities to protect lives and property from future disasters. Funding delays occurred, in part, because— (1) Louisiana's local governments had not submitted hazard mitigation plans that FEMA must review and approve to allow applicants to receive HMGP funds; (2) FEMA did not require Louisiana to submit project applications within required deadlines according to Federal regulations and FEMA policy guidance; and (3) FEMA allowed Louisiana to submit incomplete

“placeholder” project applications, despite FEMA policy that requires states to submit complete applications.

To correct this problem, FEMA and Louisiana officials need to develop a plan to accelerate their review and approval of the remaining mitigation project applications that Louisiana submitted by the final approved deadline, and de-allocate all remaining unobligated funds.

In addition, Louisiana has paid applicants about \$1 billion of the \$1.35 billion FEMA has obligated for approved HMGP projects. However, Louisiana has closed projects totaling only \$15.4 million, or 1.1 percent of the \$1.35 billion obligated. Contributing to the delay in closing HMGP projects is that neither FEMA nor Louisiana has established periods of performance for individual approved HMGP projects. Unless FEMA and Louisiana resolve this issue, hazard mitigation projects risk remaining open indefinitely, while institutional knowledge, supporting documentation, and access to records disappear with the passage of time. Accordingly, FEMA and Louisiana need to develop and implement a comprehensive strategy to complete and close all approved HMGP projects in a timely manner.

Goal 5.3: Ensure Effective Emergency Response

GAO Reports

Emergency Transportation Relief: Agencies Could Improve Collaboration Begun during Hurricane Sandy Response

Number: GAO-14-512

Date: May 28, 2014

Summary: The Department of Transportation (DOT) is in the process of allocating, obligating, and disbursing the \$13 billion appropriated by the Disaster Relief Appropriations Act, 2013 (DRAA) for surface transportation relief. Most of the DRAA surface transportation funds—over \$10 billion—were appropriated to the Federal Transit Administration’s (FTA) new Public Transportation Emergency Relief Program. An FTA damage assessment in January 2013 estimated the costs of repairing facilities damaged by Hurricane Sandy in New York and New Jersey to be about \$5.7 billion. To date, FTA has obligated about \$1.5 billion for 15 grants and disbursed about \$499 million to reimburse transit agencies for emergency response, recovery, and repair costs. These disbursements are consistent with Congressional Budget Office estimates, and transit projects can take years to complete. Furthermore, FTA plans to use nearly half of its DRAA appropriation for resiliency projects (or projects to protect facilities from future damage), most of which will be carried out through a competitive grant process. FTA was evaluating applications when GAO completed its review.

FTA’s new Public Transportation Emergency Relief Program has more flexibility and fewer restrictions in funding projects compared to the Federal Emergency Management Agency’s (FEMA) Public Assistance and Hazard Mitigation programs and the Federal Highway Administration’s (FHWA) Emergency Relief Program. For example, FEMA’s Hazard Mitigation program places limits on the amount of emergency relief funds that can be used for resiliency projects, while FTA’s program does not. FTA’s program also has more flexibility in how funds can

be used for repairs, allowing transit agencies to improve facilities beyond pre-disaster conditions. The use of emergency relief funds for projects that go beyond recovery efforts is not new—activities funded by FHWA’s Emergency Relief Program have also expanded beyond repair and reconstruction. The expanding scope of emergency relief assistance illustrates the fiscal exposure the federal government faces and the challenges of establishing long-term sustainable funding for disaster relief and recovery.

Although FTA and FEMA have a memorandum of agreement for assisting transit providers during emergencies, they are limited in their ability to delineate specific roles and responsibilities for future disasters. This limit is because while FEMA receives funding on an ongoing basis, FTA, to date, has only received a supplemental appropriation for Hurricane Sandy and does not know what resources it will have for future disasters. Because FTA and FEMA have the authority to fund many of the same activities by law, transit agencies may experience confusion when seeking assistance under some circumstances. FTA and FEMA have not determined how collaborative efforts, including their communications program and protocol contemplated in the memorandum of agreement, will be monitored, evaluated, and reported, but instead rely on informal communication. As GAO has previously concluded, creating a means to evaluate the results of collaborative efforts can enhance and sustain them, and informal communications between federal agencies do not ensure that collaboration is effective. Establishing more formal monitoring and evaluation of combined efforts could help FTA and FEMA ensure effective collaboration.

GAO recommends that DOT and the Department of Homeland Security (DHS) direct FTA and FEMA to establish specific guidelines to monitor, evaluate, and report the results of collaborative efforts—including their communications program and protocol as contemplated in their memorandum of agreement.

DHS OIG Reports

FEMA’s Dissemination of Procurement Advice Early in Disaster Response Periods

Number: [OIG-14-46-D](#)

Date: February 28, 2014

Summary: From May 18 to 20, 2013, Oklahoma City, Oklahoma, and surrounding counties experienced severe storms and tornadoes, including an EF-5 tornado that struck the City of Moore on May 20, 2013. The State of Oklahoma (State) reported 26 fatalities and more than 387 injuries as a result of these storms.² On May 20, 2013, the President declared a major disaster with an incident period beginning on May 18, 2013, and extending to June 2, 2013.

During our deployment to the Oklahoma City Joint Field Office, we observed instances where FEMA personnel provided incomplete and, at times, inaccurate information to Public Assistance applicants regarding Federal procurement standards. Based on our audit reports and personal observations, similar instances have been occurring for several years. Thus, we were not surprised when we learned that FEMA officials did not emphasize contracting compliance training at the Joint Field Office. Contracting violations significantly increase the risk that contracts for disaster work will result in ineligible and excessive costs and that open and fair competition will not occur.

Therefore, FEMA should take immediate steps to ensure that its Joint Field Office personnel provide complete and accurate information on Federal procurement standards.

FEMA Should Take Steps to Improve the Efficiency and Effectiveness of the Disaster Assistance Helpline for Disaster Survivors That Do Not Speak English or Spanish

Number: [OIG-14-118-D](#)

Date: July 29, 2014

Summary: On September 26, 2013, the Office of Inspector General deployed an Emergency Management Oversight Team (EMOT) to the Joint Field Office located in Centennial, Colorado. The EMOT serves as an independent unit for oversight of disaster response and recovery activities. It provides FEMA an additional resource for proactive evaluation to prevent and detect systemic problems in disaster programs and help ensure accountability over Federal funds. One area that we identified throughout the course of our fieldwork as being integral to FEMA's mission to support the needs of disaster survivors—and thus prudent for us to test—was FEMA's Disaster Assistance Helpline.

FEMA's Disaster Assistance Helpline could not consistently accommodate a variety of non-English/Spanish-speaking disaster survivors seeking to register for disaster aid and receive answers to their FEMA-related questions in an efficient or effective manner. Non-English/Spanish-speaking disaster survivor callers can experience challenges in applying for and/or receiving disaster assistance because they are unable to communicate with Helpline operators. Because of the important role that these operators have in interacting with disaster survivors, FEMA needs to take every cost-effective measure to ease the burden on all survivors—not just English/Spanish-speaking survivors.

FEMA translates more than a dozen disaster assistance fliers, brochures, and pamphlets into 23 different languages. However, FEMA should update those materials to prepare the non-English/Spanish-speaking survivor for the English language-related capabilities or resources they may need throughout the Helpline process. FEMA should also consider having other language-based resources available to assist operators communicating with callers who cannot speak English or Spanish.

FEMA's Logistics Supply Chain Management System May Not Be Effective During a Catastrophic Disaster

Number: [OIG-14-151](#)

Date: September 22, 2014

Summary: We audited the Federal Emergency Management Agency's (FEMA) Logistics Supply Chain Management System program. According to FEMA, the Logistics Supply Chain Management System replaced its earlier logistics operations systems to automate and track distribution better and deliver emergency supplies more dependably. FEMA also intended for the system to help track supplies provided by partners in other Federal agencies; nongovernmental organizations; state, local, and tribal governments; and the private sector. Our audit objective was to determine whether FEMA's Logistics Supply Chain Management System is able to support Federal logistics operations effectively in the event of a catastrophic disaster.

After spending about \$247 million over 9 years, FEMA cannot be certain that its supply chain management system will be effective during a catastrophic disaster. FEMA estimated that the life

cycle cost of the system would be about \$556 million—\$231 million more than the original life cycle cost estimate. According to FEMA, the Logistics Supply Chain Management System became fully operational in January 2013, which was about 19 months behind schedule. However, the system could not perform as originally planned. Specifically, it cannot interface with the logistics management systems of FEMA’s partners, nor does FEMA have real-time visibility over all supplies shipped by its partners. As of March 2014, the Logistics Supply Chain Management System still had not achieved full operational capability. We attribute these deficiencies to inadequate program management and oversight by the Department of Homeland Security (DHS) and FEMA. As a result, FEMA may not be able to efficiently and effectively aid survivors of catastrophic disaster.

We made three additional observations related to the Logistics Supply Chain Management System. FEMA may not have the appropriate number of trained and proficient staff to operate the system during a disaster. In addition, FEMA has not published system operating procedures or guidance on using other processes should the Logistics Supply Chain Management System not be available. Finally, the program office responsible for the Logistics Supply Chain Management System inaccurately reported at least three program performance measures to the Office of Management and Budget. We made 11 recommendations to address these deficiencies and observations and improve the effectiveness of the Logistics Supply Chain Management System program.

Goal 5.4: Enable Rapid Recovery

GAO Reports

Hurricane Sandy Relief: Improved Guidance on Designing Internal Control Plans Could Enhance Oversight of Disaster Funding

Number: [GAO-14-58](#)

Date: November 26, 2013

Summary: In response to the Disaster Relief Appropriations Act, 2013, agencies prepared Hurricane Sandy disaster relief internal control plans based on Office of Management and Budget (OMB) guidance but did not consistently apply the guidance in preparing these plans. OMB Memorandum M-13-07 (M-13-07), Accountability for Funds Provided by the Disaster Relief Appropriations Act, directed federal agencies to provide a description of incremental risks they identified for Sandy disaster relief funding as well as an internal control strategy for mitigating these risks. Each of the 19 agencies responsible for the 61 programs receiving funds under the act submitted an internal control plan with specific program details using a template provided by OMB. Agencies’ plans ranged from providing most of the required information to not providing any information on certain programs. For example, each of the 61 programs was required to discuss its protocol for improper payments; however, GAO found that 38 programs included this information, 11 included partial information, and 12 included no information.

National Flood Insurance Program: Progress Made on Contract Management but Monitoring and Reporting Could Be Improved**Number:** [GAO-14-160](#)**Date:** January 15, 2014

Summary: The Federal Emergency Management Agency (FEMA) has made progress in improving its processes for monitoring NFIP contracts since GAO last reported on these issues in 2008 and 2011. For example, GAO recommended in 2011 that FEMA complete the development and implementation of its revised acquisition process to be consistent with a Department of Homeland Security (DHS) directive. FEMA updated its contract management guidance and revised its handbook for contracting officer's representatives to be consistent with DHS directives. The updated handbook also contained many of the elements identified in a federal guide to best practices for contract administration. Furthermore, the FEMA division that manages the National Flood Insurance Program (NFIP) developed a contract management reference guide that followed FEMA's handbook and federal best practices guidance.

With some exceptions, FEMA largely followed its contract monitoring procedures for the three largest NFIP contractors GAO reviewed. To improve monitoring and reporting of contractor performance, we are recommending that FEMA (1) determine the extent to which quality assurance surveillance plans and CPARS assessments have not been prepared, (2) identify the reasons why, and (3) take steps, as needed, to address those reasons. FEMA concurred with GAO's recommendations.

Flood Insurance: Strategies for Increasing Private Sector Involvement**Number:** [GAO-14-127](#)**Date:** January 22, 2014

Summary: According to stakeholders with whom GAO spoke, several conditions must be present to increase private sector involvement in the sale of flood insurance. First, insurers need to be able to accurately assess risk to determine premium rates. For example, stakeholders told GAO that access to National Flood Insurance Program (NFIP) policy and claims data and upcoming improvements in private sector computer modeling could enable them to better assess risk. Second, insurers need to be able to charge premium rates that reflect the full estimated risk of potential flood losses while still allowing the companies to make a profit, as well as be able to decide which applicants they will insure. However, stakeholders said that such rates might seem unaffordable to many homeowners. Third, insurers need sufficient consumer participation to properly manage and diversify their risk, but stakeholders said that many property owners do not buy flood insurance because they may have an inaccurate perception of their risk of flooding.

Stakeholders identified several strategies that could help create conditions that would promote the sale of flood insurance by the private sector. For example,

- **NFIP charging full-risk rates.** Congress could eliminate subsidized rates, charge all policyholders full-risk rates, and appropriate funding for a direct means-based subsidy to some policyholders. Stakeholders said full-risk NFIP rates would encourage private sector participation because they would be much closer to the rates private insurers would need to charge. The explicit subsidy would address affordability concerns, increase transparency, and reduce taxpayer costs depending on the extent and amount of the subsidy. The Biggert-Waters Act eliminates some subsidized rates, but some have proposed delaying these rate

increases. Doing so could address affordability concerns, but would also delay addressing NFIP's burden on taxpayers.

- **NFIP providing residual insurance.** The federal government could also encourage private sector involvement by providing coverage for the highest-risk properties that the private sector is unwilling to insure. Providing residual coverage could increase the program's exposure relative to the number of properties it insured, but NFIP would be insuring fewer properties, and charging adequate rates could reduce taxpayer costs.
- **NFIP as reinsurer.** Alternatively, the federal government could serve as a reinsurer, charging a premium for assuming the risk of catastrophic losses. However, the cost of reinsurance premiums would likely be passed on to consumers, with higher rates potentially decreasing consumer participation.

Stakeholders identified other strategies including mandatory coverage requirements to ensure broad participation, NFIP purchasing reinsurance from the private sector rather than borrowing from the U.S. Treasury, and NFIP issuing catastrophe bonds to transfer risk to private investors. As the private sector increases its role in providing flood coverage, the federal government could collaborate with state and local governments to focus on other important roles, including promoting risk awareness among consumers, encouraging mitigation, enforcing building codes, overseeing land use agreements, and streamlining insurance regulations.

While GAO makes no new recommendations in this report, GAO reiterates its previous suggestion from a June 2011 report (GAO-11-297) that Congress consider eliminating subsidized rates, charge full-risk rates to all policyholders, and appropriate funds for premium assistance to eligible policyholders to address affordability issues.

Mature and Strengthen Homeland Security

Goal: Integrate Intelligence, Information Sharing, and Operations

GAO Reports

DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges

Number: [GAO-14-397](#)

Date: June 4, 2014

Summary: DHS has established mechanisms to better integrate analysis activities throughout the department, but the mechanisms are not functioning as intended. According to officials from DHS' Office of Intelligence and Analysis (I&A), it can be challenging for DHS components to focus on developing both strategic priorities and more tactical priorities that support their specific operations. Absent strategic priorities, DHS used component subject matter experts and other information to develop key questions of common interest they would address through analysis. As a result, DHS does not have reasonable assurance that component analytic activities and resource investments are aligned to support departmental priorities.

I&A has taken steps to address challenges it faced in maintaining a skilled workforce, but has not assessed whether its efforts are resolving the challenges. For example: I&A faced challenges in recruiting and hiring analysts, in part because of its hiring authority, which put it at a disadvantage compared with other agencies that were able to process hiring actions more quickly. I&A's hiring authority was changed in 2013, a fact that could help ease these challenges. I&A experienced low morale and high rates of attrition, particularly among its lower-level analysts. To help address these issues, I&A restructured its grade levels in 2012 to provide additional career advancement opportunities.

However, I&A has not established mechanisms to evaluate its efforts and use the results to make any needed changes because I&A leadership has focused on other priorities. Such mechanisms will help I&A evaluate if efforts are achieving their intended results of improving recruiting and hiring, bolstering morale, and reducing attrition. In addition, using the evaluation results to determine any needed changes will help ensure that I&A is making sound workforce decisions.

GAO recommends, among other things, that DHS (1) establish strategic intelligence priorities and use them to inform analytic activities and (2) establish mechanisms to evaluate workforce initiatives and use results to determine any needed changes. DHS concurred with our recommendations.

DHS OIG Reports

Lessons Learned from the Boston Marathon Bombing: Improving Intelligence and Information Sharing

Number: [Testimony](#)

Date: April 10, 2014

Summary: DHS has built close relationships with partners in communities across the Nation and improved its support to them, actions that will continue to make America stronger and more resilient to terrorist attacks, and threats and hazards of all kinds. DHS works with first responders, law enforcement, individuals, private sector partners, and communities across the country to reduce vulnerabilities and enhance preparedness while strengthening emergency response capabilities at the Federal, State, local, tribal and territorial levels. While America is stronger and more resilient as a result of efforts over the past decade to build robust national capabilities, the Boston Marathon bombings serve as a reminder that threats from terrorism persist and continue to evolve.

Since the Boston attack, DHS, the Federal Bureau of Investigation (FBI), and National Counterterrorism Center (NCTC) have expanded information sharing with state and local officials about potential threats. DHS also sent updated guidance to officers at the Joint Terrorism Task Force (JTTF) to improve on our strong foundation of collaboration with the FBI. Additionally, DHS also continues to work closely with federal partners to screen and vet domestic and international travelers, visa applicants and other persons of interest to identify potential threats.

DHS is pleased to note OIG's recognition that the Department and its external partners generally shared information and followed procedures appropriately. For example, as stated in the draft report, U.S. Customs and Border Protection (CBP) followed the appropriate policy and procedures during the outbound and inbound vetting of Tamerlan Tsarnaev's travel.

CBP continuously strives to improve its processes while ensuring that information provided is accurate and verified. For example, CBP established a "formalized notification procedure" to ensure documentable communication in the fast-paced environment of the JTTF.

The draft report contained one recommendation: The Federal Bureau of Investigation and DHS clarify the circumstances under which Joint Terrorism Task Force personnel may change the display status of a TECS record, particularly in closed cases.

Goal: Enhance Partnerships and Outreach

No GAO of DHS OIG reports were available that aligned to this goal.

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

No GAO of DHS OIG reports were available that aligned to this goal.

Goal: Conduct Homeland Security Research and Development

GAO Reports

Department of Homeland Security: Continued Actions Needed to Strengthen Oversight and Coordination of Research and Development

Number: [GAO-14-813T](#)

Date: July 31, 2014

Summary: In September 2012, GAO reported that the Department of Homeland Security (DHS) did not know the total amount its components invested in research and development (R&D) and did not have policies and guidance for defining R&D and overseeing R&D resources across the department. According to DHS, its Science & Technology Directorate (S&T), Domestic Nuclear Detection Office (DNDO), and Coast Guard were the only components that conducted R&D, and GAO found that these were the only components that reported budget authority, obligations, or outlays for R&D activities to the Office of Management and Budget. However, GAO identified an additional \$255 million in R&D obligations made by other DHS components. At the time of GAO's review, DHS reported it was difficult to identify all R&D investments across the department because DHS did not have a department wide policy defining R&D or guidance directing components how to report all R&D activities. GAO recommended that DHS develop policies to assist components in better understanding how to report R&D activities and better position DHS to determine R&D investments. DHS concurred with the recommendation and, as of July 2014, had updated its guidance to include a definition of R&D but had not yet determined the most effective path to guide R&D across the department. GAO will continue to monitor DHS's efforts to develop its approach for overseeing R&D at the department.

GAO also reported in September 2012 that S&T had taken some steps to coordinate R&D efforts across DHS, but the department's R&D efforts were fragmented and overlapping, which increased the risk of unnecessary duplication. GAO recommended that DHS develop a policy defining roles and responsibilities for coordinating R&D and establish a mechanism to track all R&D projects to help DHS mitigate existing fragmentation and overlap and reduce the risk of unnecessary duplication. DHS concurred with the recommendation. As of July 2014, S&T has not developed new policy guidance but is conducting portfolio reviews across the department.

In September 2013, GAO reported that DHS border and maritime R&D components reported producing 97 R&D deliverables from fiscal year 2010 through 2012 at an estimated cost of \$177 million. GAO found that the type of border and maritime R&D deliverables produced by S&T, the Coast Guard, and DNDO varied, and R&D customers GAO met with had mixed views on the impact of the deliverables. For example, S&T developed prototype radar and video systems for use by Border Patrol. However, GAO reported that S&T had not established timeframes for collecting and evaluating feedback on the extent to which deliverables met customers' needs. GAO recommended that S&T collect such feedback from its customers to better determine the usefulness and impact of its R&D projects and deliverables and make better-informed decisions regarding future work. As of July 2014, DHS had taken steps to address this recommendation, including making plans to gather customer feedback.

In its prior reports, GAO recommended, among other things, that DHS develop policies and guidance for defining, overseeing, coordinating, and tracking R&D activities across the department; and that S&T collect and evaluate feedback from its customers. DHS concurred with GAO's recommendations and has actions underway to address them.

Goal: Ensure Readiness of Frontline Operators and First Responders

GAO Reports

Improved Documentation, Resource Tracking, and Performance Measurement Could Strengthen Efforts

Number: [GAO-14-688](#)

Date: September 10, 2014

Summary: The Department of Homeland Security (DHS) has processes to evaluate training, track resources, and assess leader development. However, various actions could better position the department to maximize the impact of its training efforts.

Training evaluation: All five DHS components in GAO's review—U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, the U.S. Coast Guard, the Transportation Security Administration, and the Federal Law Enforcement Training Center—have a documented process to evaluate their training programs. Their documented processes fully included three of six attributes of effective training evaluation processes identifying goals, programs to evaluate, and how results are to be used. However, the documented processes did not consistently include the other three attributes: methodology, timeframes, and roles and responsibilities. By updating documentation to address these attributes, DHS components would have more complete information to guide its efforts in conducting effective evaluations.

Capturing training cost: DHS identified efficiencies and cost savings for delivering a number of training programs. However, different methods are used for capturing training costs across the department, which poses challenges for reliably capturing these costs across DHS. Components capture training costs differently, contributing to inconsistencies in training costs captured across DHS. Variation in methods used to collect data can affect the reliability and quality of DHS-wide training program costs. However, DHS has not identified all challenges that contribute to these inconsistencies. DHS could improve its awareness about the costs of training programs DHS-wide and thereby enhance its resource stewardship by identifying existing challenges that prevent DHS from accurately capturing training costs and implementing corrective measures.

Leader development: DHS's Leader Development Program (LDP) Office is in the process of implementing a department-wide framework to build leadership skills. However, the LDP Office has not clearly identified program goals and the measures it uses to assess program effectiveness do not exhibit some attributes that GAO previously identified as key for successful performance measurement. These include linkage of performance measures to the program's goals, clarity, and establishment of measurable targets to assess the measures. By clearly identifying program goals and incorporating key attributes, the LDP could better ensure actionable information for identifying and making program improvements.

GAO recommends that DHS update its documentation to fully reflect key attributes of an effective evaluation, identify challenges to and corrective measures for capturing training costs department-wide, and clearly identify LDP goals and ensure that LDP performance measures reflect key attributes.

Goal: Strengthen Service Delivery and Manage DHS Resources

GAO Reports

DHS Financial Management: Continued Effort Needed to Address Internal Control and System Challenges

Number: [GAO-14-106T](#)

Date: November 15, 2013

Summary: GAO reported that the Department of Homeland Security (DHS) had made considerable progress toward obtaining a clean opinion on its financial statements; reducing the number of audit qualifications from 11 in 2005 to 1 in 2010. GAO also reported that DHS had made limited progress in establishing effective controls to obtain a clean opinion on its internal control over financial reporting. Although the number of auditor-reported material weaknesses in DHS' internal control over financial reporting has decreased from 10 in 2005 to 5 in 2011, DHS' auditors reported five material weaknesses for fiscal year 2012. Lastly GAO reported that DHS is in the early planning stages of implementing its decentralized approach for modernizing its components' financial systems, with each component determining the specific solution for its financial systems modernization. GAO is not making any new recommendations. However, GAO's September 2013 report included two recommendations to DHS regarding the need to follow IT best practices related to its target state and transition plan. DHS generally agreed with the recommendations and described actions already taken, but GAO believes that further action is needed to address them. GAO also had two other findings and recommendations related to IT best practices and the need for DHS, at the time of GAO's review, to update its standard operating procedures and include specific procedures for its integrated master schedule and lessons learned process. GAO agreed that DHS completed actions to address these two recommendations after receiving the draft report for comment.

DHS Management and Administration Spending: Reliable Data Could Help DHS Better Estimate Resource Requests

Number: [GAO-14-27](#)

Date: December 4, 2013

Summary: Officials from all eight Department of Homeland Security (DHS) components in GAO's review define management and administration (M&A) activities--activities that help agencies achieve their mission and program goals--differently, and while component officials said they can identify M&A spending, limitations exist in obtaining spending data from fiscal years 1999 through 2013. Officials from four of the eight components define their M&A activities according to the activities funded through their appropriations accounts and programs, projects, or activities (PPA) that are M&A in nature. The remaining four components each define M&A activities differently, and those definitions are not tied to activities contained in specific appropriations accounts. According to component officials, the eight components GAO reviewed can identify their

M&A spending, but currently do not because they are not required to do so by the department. Because components define M&A differently, have different methods for identifying spending, and limitations exist in obtaining data, it is not possible to compare components' M&A spending data from fiscal years 1999 through 2013.

DHS has not identified the department's total spending on M&A activities and has encountered difficulties in implementing steps to define and collect data on M&A activities. Specifically, in 2010, DHS developed a common definition of M&A in conjunction with the Future Years Homeland Security Program (FYHSP) System Program Data Module (PDM) for components to submit resource allocation requests for future years by activity type: mission/operational, mission support, and business support/M&A. However, DHS is unable to reliably estimate what percentage of its requests are identified as M&A because 4 out of 15 components did not enter all appropriate business support/M&A activities and 1 component did not enter any business support/M&A activities, among other errors, which DHS officials said are a result of manual data entry and components not adhering to the guidance in the user manual. DHS does not have a mechanism in place to work with the components to correct data errors in the FYHSP System PDM. By implementing a mechanism to assess whether components have entered the appropriate M&A activities into the PDM, and working with the components to correct the data, as needed, DHS would be better positioned to reliably estimate and report to external stakeholders what percentage of DHS's resource allocations requests are identified as M&A.

GAO recommends that DHS implement a mechanism to assess and correct M&A data entered by components into the PDM. DHS concurred with GAO's recommendation.

Department of Homeland Security: DHS's Efforts to Improve Employee Morale and Fill Senior Leadership Vacancies

Number: [GAO-14-228T](#)

Date: December 12, 2013

Summary: In September 2012, GAO reported that Department of Homeland Security (DHS) employees identified having lower average morale than the average for the rest of the federal government, but morale varied across components. Specifically, GAO found that, according to the Office of Personnel Management's 2011 Federal Employee Viewpoint Survey (FEVS), DHS employees had 4.5 percentage points lower job satisfaction and 7.0 percentage point lower engagement--the extent to which employees are immersed in their work and spending extra effort on job performance. In September 2012, GAO recommended that DHS take action to better determine the root cause of low employee morale, and where absent, add benchmarking against similar organizations, among other things. Since September 2012, DHS has taken a number of actions intended to improve employee morale, such as directing component human capital officials to reevaluate their action plans to ensure that metrics of success are clear and measurable. In December 2013, GAO found that DHS has actions underway to address GAO's recommendations but DHS has not fully implemented them. It will be important to do so, as DHS employee job satisfaction declined in fiscal years 2012 and 2013 FEVS results. Specifically, 2013 FEVS data show that DHS employee satisfaction decreased 7 percentage points since 2011, which is more than the government-wide decrease of 4 percentage points over the same time period. As a result, the gap between average DHS employee satisfaction and the government-wide average widened to 7 percentage points. DHS has also consistently scored lower than the government-wide average on the FEVS Leadership and Knowledge Management index, which indicates the extent to which

employees hold their leadership in high regard. Since 2011, DHS's scores for this index have decreased 5 percentage points, widening the gap between the DHS average and the government-wide average to 9 percentage points.

In February 2012, GAO reported that DHS Senior Executive Service (SES) vacancy rates, while reaching a peak of 25 percent in 2006, had generally declined, reaching 10 percent at the end of fiscal year 2011. GAO also reported that component officials identified a number of factors that may have contributed to component SES vacancy rates during that time period, including increases in SES allocations, events like presidential transitions, and organizational factors such as reorganizations. To help reduce SES vacancy rates, DHS has (1) implemented a simplified pilot hiring process aimed at attracting additional qualified applicants and planned to expand the method for all SES, and (2) implemented a centralized SES candidate development program aimed at providing a consistent approach to leadership training. As of December 2013, DHS had made the pilot process available to all components, but had not yet performed analysis of these efforts' effectiveness at reducing SES vacancy rates which, according to DHS data, have remained relatively steady since GAO's February 2012 report--11 percent at the end of fiscal year 2013.

GAO has made recommendations in prior reports for DHS to strengthen its analysis of low employee morale, and identify clear and measurable metrics for action plan success. DHS concurred with these recommendations and has reported actions under way to address them. GAO provided a copy of new information in this statement to DHS for review. DHS confirmed the accuracy of this information.

Strategic Sourcing: Selected Agencies Should Develop Performance Measures on Inclusion of Small Businesses and OMB Should Improve Monitoring

Number: [GAO-14-126](#)

Date: January 23, 2014

Summary: The Office of Management and Budget (OMB), the General Services Administration (GSA), and selected agencies have taken steps to consider small businesses, including small disadvantaged businesses, in their strategic sourcing efforts. (Small disadvantaged businesses are those unconditionally owned and controlled by socially and economically disadvantaged individuals.) OMB and GSA have developed guidance on strategic sourcing that stresses the importance of including small businesses. GAO's review of agency-wide strategic sourcing initiatives at each of five agencies--Departments of Defense (DOD), Homeland Security (DHS); Housing and Urban Development (HUD); and the Interior and the National Aeronautics and Space Administration (NASA)--showed that the agencies generally considered the inclusion of small businesses.

Data and performance measures that would provide a more precise understanding of the inclusion of small and disadvantaged businesses in strategic sourcing initiatives are limited. DHS has collected some data on contracts awarded to small businesses under strategic sourcing initiatives, but it and the other agencies in GAO's review generally did not have baseline data and performance measures to determine how small businesses were affected by strategic sourcing. Without baseline data and performance measures, the effect of strategic sourcing initiatives on small businesses will be difficult to determine. Moreover, OMB has not monitored agencies' compliance in reporting baseline data and performance measures on the inclusion of small businesses in government-wide and agency-wide strategic sourcing initiatives. OMB required agencies to submit annual reports on

the implementation of strategic sourcing from fiscal years 2005 through 2007 and prepare information for acquisition status sessions from fiscal years 2010 through 2012. (No reporting was in place for fiscal years 2008 or 2009.) However, virtually none of this information included baseline data or measures of the effect of strategic sourcing on small businesses. Without effective monitoring, it will be difficult for OMB to help ensure that agencies are tracking the impact of strategic sourcing on small businesses.

GAO makes recommendations to DHS to improve data collection and performance measures related to the inclusion of small businesses in strategic sourcing. DHS agreed with GAO's recommendation.

Homeland Security Acquisitions: DHS Could Better Manage Its Portfolio to Address Funding Gaps and Improve Communications with Congress

Number: [GAO-14-332](#)

Date: April 17, 2014

Summary: GAO found that the funding plans for all 35 of the Department of Homeland Security (DHS) acquisition programs it reviewed changed to some degree from fiscal years 2012 to 2014. Program officials reported that funding instability negatively affected 17 of the 35 programs, contributing to schedule slips, cost growth, and capability reductions. DHS officials at headquarters, components, and program offices identified internal and external factors that contributed to funding instability. These included changes in department-wide priorities and congressional funding decisions. Going forward, DHS's largest acquisition programs will likely experience more funding instability because the department's plans for its acquisition portfolio are not currently affordable. Nevertheless, the department has not approved most of its major acquisition programs' cost estimates. As a result, DHS's understanding of its major acquisition programs' funding requirements is limited, and the funding gap may be greater than the department has suggested.

DHS has not consistently developed its multi-year funding plans in accordance with key portfolio management practices that would help the department optimize the return on its acquisition investments. DHS's resource allocation guidance reflects some but not all of these key practices and the department is working to address the shortfalls. To help address its funding issues, the department is piloting a four-pronged portfolio management initiative intended to provide a framework for information to flow between four key councils and boards. There are opportunities for DHS leadership to improve governance, but senior DHS officials do not expect the initiative will be fully implemented in the near term, so it is too soon to tell how effective it will be. DHS has met statutory reporting requirements for its major acquisition programs' multi-year funding plans through its annual Future Years Homeland Security Program reports. However, the department has opportunities to improve how it communicates its acquisition funding needs to Congress in the future. Most notably, DHS does not currently link its major acquisition programs to the homeland security strategy, and its annual report does not identify acquisition programs' funding gaps. Adding this information would provide Congress valuable insights into DHS's acquisition funding needs.

GAO recommends DHS take nine actions to better manage its portfolio and improve communications with Congress. DHS concurred with GAO's recommendations and stated that it

addressed one in March 2014. DHS presented plans to address the other eight, but GAO does not believe the plan for one of them is fully responsive.

Information Technology: Agencies Need to Establish and Implement Incremental Development Policies

Number: [GAO-14-361](#)

Date: May 1, 2014

Summary: All five agencies in GAO's review—the Departments of Defense (Defense), Health and Human Services (HHS), Homeland Security (DHS), Transportation (Transportation), and Veterans Affairs (VA)—have established policies that address incremental development; however, the policies usually did not fully address three key components for implementing the Office of Management and Budget's (OMB) guidance. Among other things, agencies cited the following reasons that contributed to these weaknesses: (1) the guidance was not feasible because not all types of investments should deliver functionality in 6 months, and (2) the guidance did not identify what agencies' policies are to include or time frames for completion. GAO agrees these concerns have merit. Until OMB issues realistic and clear guidance and agencies address the weaknesses in their incremental development policies, it will be difficult to deliver project capability more rapidly. GAO recommends that DHS modify, finalize, and implement policies governing incremental development to ensure that those policies comply with OMB's guidance, once that guidance is made available.

Department of Homeland Security: Progress Made; Significant Work Remains in Addressing High-Risk Areas

Number: [GAO-14-532T](#)

Date: May 7, 2014

Summary: The Department of Homeland Security (DHS) has made progress in addressing high-risk areas for which it has sole responsibility, but significant work remains.

Strengthening management functions. In this area, DHS has met two and partially met three of GAO's five criteria for removing areas from the high-risk list. Specifically, DHS has met the criteria for having (1) demonstrated leadership commitment, and (2) a corrective action plan for addressing its management risks. However, it has partially met GAO's criteria for (1) capacity (having sufficient resources); (2) having a framework to monitor progress; and (3) demonstrated, sustained progress. DHS has made important progress, but to more fully address GAO's high-risk designation, DHS needs to show measurable, sustainable progress in implementing key management initiatives.

National Flood Insurance Program (NFIP). DHS's FEMA, which manages the NFIP, has partially met the five criteria for NFIP removal from the high-risk list, but needs to initiate or complete additional actions. For example, FEMA has not completed actions in certain areas, such as modernizing its claims and policy management system and overseeing compensation of insurers that sell NFIP policies. In addition, FEMA is unlikely to generate sufficient revenue to cover future catastrophic losses or repay billions of dollars borrowed from the Department of the Treasury. As of December 2013, FEMA owed the Treasury \$24 billion—primarily to pay claims associated with Superstorm Sandy (2012) and Hurricane Katrina (2005)—and had not made a principal payment since 2010.

Progress has been made in the following government-wide high-risk areas in which DHS plays a critical role, but significant work remains.

Information security and cyber critical infrastructure protection. Federal agencies, including DHS, have taken a variety of actions that were intended to enhance federal and critical infrastructure cybersecurity, but more efforts are needed. DHS needs to take several actions to better oversee and assist agencies in improving information security practices. For instance, DHS should continue to assist agencies in developing and acquiring continuous diagnostic and mitigation capabilities to protect networks and counteract day-to-day cyber threats. In addition, DHS has taken steps to enhance the protection of cyber critical infrastructure but could do more to enhance coordination with the private sector.

Terrorism-related information sharing. The federal government faces significant challenges in sharing terrorism-related information. However, DHS has made significant progress in enhancing the sharing of this information. For example, DHS is taking steps to measure the extent to which fusion centers—collaborative efforts within states that investigate and respond to criminal and terrorist activity—are coordinating with other field-based task forces and centers to share terrorism-related information, and assessing opportunities to improve coordination and information sharing. The federal government has important work ahead to address the high risk issue, such as developing metrics that measure the homeland security results achieved from improved information sharing. GAO has made over 2,100 recommendations to DHS since its establishment in 2003 to strengthen its management and integration efforts, among other things. DHS has implemented more than 65 percent of these recommendations and has actions under way to address others.

Coast Guard Acquisitions: Better Information on Performance and Funding Needed to Address Shortfalls

Number: [GAO-14-450](#)

Date: June 5, 2014

Summary: The selected Coast Guard assets that GAO reviewed are generally demonstrating improved performance—according to Coast Guard operators—but GAO found that they have yet to meet all key requirements. Specifically, two assets, the HC-144 patrol aircraft and Fast Response Cutter, did not meet all key requirements during operational testing before being approved for full-rate production, and Department of Homeland Security (DHS) and Coast Guard guidance do not clearly specify when this level of performance should be achieved. Additionally, the Coast Guard changed its testing strategy for the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) system and, as a result, is no longer planning to test the system’s key requirements. Completing operational testing for the C4ISR system would provide the Coast Guard with the knowledge of whether this asset meets requirements.

As acquisition program costs increase across the portfolio, consuming significant amounts of funding, the Coast Guard is farther from fielding its planned fleet today than it was in 2009, in terms of the money needed to finish these programs. In 2009, GAO found that the Coast Guard needed \$18.2 billion to finish its 2007 baseline, but now needs \$20.7 billion to finish these assets.

To inform Congress of its budget plans, the Coast Guard uses a statutorily required 5-year Capital Investment Plan, but the law does not require the Coast Guard to report the effects of actual funding levels on individual projects and, thus, it has not done so. For example, the Coast Guard has

received less funding than planned in its annual budgets, but has not reflected the effects of this reduced funding in terms of increased cost or schedule for certain projects. Without complete information, Congress cannot know the full cost of the portfolio.

The Coast Guard has repeatedly delayed and reduced its capability through its annual budget process and, therefore, it does not know the extent to which it will meet mission needs and achieve desired results. This is because the Coast Guard does not have a long-term fleet modernization plan that identifies all acquisitions needed to meet mission needs over the next two decades within available resources. Without such a plan, the Coast Guard cannot know the extent to which its assets are affordable and whether it can maintain service levels and meet mission needs.

Congress should consider requiring the Coast Guard to include additional information in its Capital Investment Plan. In addition, the Secretary of DHS should clarify when minimum performance standards should be achieved, conduct C4ISR testing, and develop a long-term modernization plan. DHS concurred with the recommendations, but its position on developing a long-term plan does not fully address GAO's concerns as discussed in the report.

Information Security: Agencies Need to Improve Oversight of Contractor Controls

Number: [GAO-14-612](#)

Date: August 8, 2014

Summary: Although the six federal agencies that GAO reviewed (the Departments of Energy (DOE), Homeland Security (DHS), State, and Transportation (DOT), the Environmental Protection Agency (EPA) and the Office of Personnel Management (OPM)) generally established security and privacy requirements and planned for assessments to determine the effectiveness of contractor implementation of controls, with the exception of DHS the agencies reviewed were inconsistent in overseeing the execution and review of those assessments, resulting in security lapses.

A contributing reason for these shortfalls is that agencies had not documented procedures for officials to follow in order to effectively oversee contractor performance. Until these agencies develop, document, and implement specific procedures for overseeing contractors, they will have reduced assurance that the contractors are adequately securing and protecting agency information.

The Office of Management and Budget (OMB), the National Institute of Standards and Technology, and the General Services Administration have developed guidance to assist agencies in ensuring the implementation of security and privacy controls by their contractors. However, OMB guidance to agencies for categorizing and reporting on contractor-operated systems is not clear on when an agency should identify a system as contractor-operated and therefore agencies are interpreting the guidance differently. In fiscal year 2012, inspectors general from 9 of the 24 major agencies found data reliability issues with agencies' categorization of contractor-operated systems. Without accurate information on the number of contractor-operated systems, OMB assistance to agencies to help improve their cybersecurity posture will be limited and OMB's report to Congress on the implementation of the Federal Information Security Management Act (FISMA) is not complete.

GAO determined that DHS has developed procedures for the oversight of contractors and has no further recommendations for DHS.

Personnel Security Clearances: Additional Guidance and Oversight Needed at DHS and DOD to Ensure Consistent Application of Revocation Process**Number:** [GAO-14-640](#)**Date:** September 8, 2014

Summary: The Department of Homeland Security (DHS) and the Department of Defense (DOD) both have systems that track varying levels of detail related to revocations of employees' security clearances. DHS's and DOD's data systems could provide data on the number of and reasons for revocations, but they could not provide some data, such as the number of individuals who received a proposal to revoke their eligibility for access to classified information, which means that the total number of employees affected by the revocation process is unknown.

Inconsistent implementation of the requirements in the governing executive orders by DHS, DOD, and some of their components, and limited oversight over the revocation process, have resulted in some employees experiencing different protections and processes than other employees. Specifically, DHS and DOD have implemented the requirements for the revocation process contained in Executive Orders 12968 and 10865 in different ways for different groups of personnel. Although certain differences are permitted or required by the executive orders, GAO found that implementation by some components could potentially be inconsistent with the executive orders in two areas. As a result, some employees may not be provided with certain information upon which a revocation appeal determination is based, and may not be told that they have a right to counsel. These inconsistencies in implementation may be in part because neither DHS nor DOD have evaluated the quality of their processes or developed performance measures to measure quality department-wide. Similarly, the Office of the Director of National Intelligence (ODNI) has only exercised limited oversight by reviewing policies and procedures within some agencies. ODNI has not established any metrics to measure the quality of the process government-wide and has not reviewed revocation processes across the federal government to determine the extent to which policies and procedures should be uniform.

DHS and DOD employees whose clearances were revoked may not have consistent employment outcomes, such as reassignment or termination, because these outcomes are determined by several factors, such as the agency's mission and needs and the manager's discretion. Further, most components could not readily ascertain employment outcomes of individuals with revoked clearances, because these data are not readily available, and communication between personnel security and human capital offices at the departments varies.

GAO recommends that DHS take several actions to improve data quality and oversight related to the personnel security revocation process. DHS generally agreed with GAO's recommendations.

Federal Real Property: DHS and GSA Need to Strengthen the Management of DHS Headquarters Consolidation**Number:** [GAO-14-648](#)**Date:** September 19, 2014

Summary: The Department of Homeland Security (DHS) and General Services Administration (GSA) planning for the DHS headquarters consolidation does not fully conform with leading capital decision-making practices intended to help agencies effectively plan and procure assets. DHS and GSA officials reported that they have taken some initial actions that may facilitate consolidation planning in a manner consistent with leading practices, such as adopting recent workplace standards

at the department level and assessing DHS's leasing portfolio. For example, DHS has an overall goal of reducing the square footage allotted per employee across DHS in accordance with current workplace standards. Officials acknowledged that this could allow more staff to occupy less space than when the campus was initially planned in 2009. DHS and GSA officials also reported analyzing different leasing options that could affect consolidation efforts. However, consolidation plans, which were finalized between 2006 and 2009, have not been updated to reflect these changes. According to DHS and GSA officials, the funding gap between what was requested and what was received from fiscal years 2009 through 2014, was over \$1.6 billion. According to these officials, this gap has escalated estimated costs by over \$1 billion—from \$3.3 billion to the current \$4.5 billion—and delayed scheduled completion by over 10 years, from an original completion date of 2015 to the current estimate of 2026. However, DHS and GSA have not conducted a comprehensive assessment of current needs, identified capability gaps, or evaluated and prioritized alternatives to help them adapt consolidation plans to changing conditions and address funding issues as reflected in leading practices. DHS and GSA reported that they have begun to work together to consider changes to their plans, but as of August 2014, they had not announced when new plans will be issued and whether they would fully conform to leading capital decision-making practices to help plan project implementation.

DHS and GSA did not follow relevant GSA guidance and GAO's leading practices when developing the cost and schedule estimates for the St. Elizabeths project, and the estimates are unreliable. For example, GAO found that the 2013 cost estimate—the most recent available—does not include a life-cycle cost analysis of the project, including the cost of operations and maintenance; was not regularly updated to reflect significant program changes, including actual costs; and does not include an independent estimate to help track the budget, as required by GSA guidance. Also, the 2008 and 2013 schedule estimates do not include all activities for the government and its contractors needed to accomplish project objectives. GAO's comparison of the cost and schedule estimates with leading practices identified the same concerns, as well as others. For example, a sensitivity analysis has not been performed to assess the reasonableness of the cost estimate. For the 2008 and 2013 schedule estimates, resources (such as labor and materials) are not accounted for and a risk assessment has not been conducted to predict a level of confidence in the project's completion date. Because DHS and GSA project cost and schedule estimates inform Congress's funding decisions and affect the agencies' abilities to effectively allocate resources, there is a risk that funding decisions and resource allocations could be made based on information that is not reliable or is out of date.

GAO recommends, among other things, that DHS and GSA develop revised DHS headquarters plans that reflect leading practices for capital decision making and reliable cost and schedule estimates. Congress should consider making future funding for the project contingent upon DHS and GSA developing plans and estimates commensurate with leading practices.

Inspectors General: DHS OIG's Structure, Policies, and Procedures Are Consistent with Standards, but Areas for Improvement Exist

Number: [GAO-14-726](#)

Date: September 24, 2014

Summary: During fiscal years 2012 and 2013, the Department of Homeland Security's (DHS) Office of Inspector General (OIG) issued 361 audit and inspection reports that collectively cover key components, management challenges identified by the OIG, and relevant high-risk areas

identified by GAO. Of the 361 reports, 200 pertained solely to the Federal Emergency Management Agency (FEMA)—the DHS component with the largest budget. Of those FEMA reports, 118 reports involved audits of disaster assistance grants.

The OIG's organizational structure, roles, and responsibilities are generally consistent with the Inspector General (IG) Act of 1978, as amended (IG Act). In 2013, the OIG made changes to its structure to enhance independence and oversight, including establishing an Office of Integrity and Quality Oversight. However, areas for improvement exist for the OIG to better meet its responsibilities.

- The OIG has not reached agreement with the Federal Bureau of Investigation (FBI) on coordinating and sharing border corruption information. The IG Act requires OIGs to recommend policies for and to conduct, supervise, or coordinate relationships with other federal agencies regarding cases of fraud or abuse. The Senate Appropriations Committee directed DHS to report jointly with the OIG and other DHS components on plans for working with the FBI.
- The OIG lacks adequate controls to protect identities of employees filing complaints because its process for recording complaints involves significant manual procedures, without review, that can be subject to human error. The IG Act requires that OIGs not disclose the identity of an employee filing a complaint without the employee's consent unless such disclosure is unavoidable during the course of an investigation. The OIG is aware of these issues and is developing standard operating procedures.
- The OIG does not have a policy for obtaining legal advice from its own counsel or guidelines specifying when it is appropriate to consult with the department's counsel. The former Acting IG requested legal help from a counsel at the department for 4 months, and it was not clear if this request was for appropriate matters. The IG Act requires the IG to obtain legal advice from a counsel reporting directly to the IG or another IG. The OIG Deputy Counsel has asked a working group to draft guidelines on consultations with the department's counsel.

The OIG's policies and procedures are consistent with independence standards. However, OIG senior executives did not always comply with the policy to annually complete certificates of independence. Because the OIG does not centrally maintain the certifications, management's ability to monitor compliance is hindered. For example, no certificate of independence could be found for the former Acting IG. As a result of an impairment to the former Acting IG's independence that was not identified in a timely manner, the OIG had to reissue six reports for fiscal year 2012 to add an explanatory statement about the impairment. External peer reviews of the OIG's audit function, completed in 2009 and 2012, also found that OIG staff, including senior executives, had not documented their independence as required.

GAO is making three recommendations for improving controls over processing complaints, obtaining legal advice, and monitoring compliance with independence standards.

DHS OIG Reports

DHS Financial Management: Investigating DHS' Stewardship of Taxpayer Dollars

Number: [Testimony](#)

Date: November 15, 2013

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

According to DHS' Office of Financial Management, in FY 2012, there was improved access to and better quality of financial management information. The Department implemented business intelligence tools to help organize, store, and analyze data more efficiently. According to the Office of Financial Management, the Department was able to take information from individual budgets and display it for the enterprise, allowing views of DHS' budget allocation by mission area. Additionally, the Department reported it was developing the Decision Support Tool to help compile department-wide program cost information and to provide a central dashboard with key indicators, such as cost, funding, and schedule, to assess and track the health of acquisitions.

Sound financial practices and related management operations are critical to achieving the Department's mission and to providing reliable, timely financial information to support management decision-making throughout DHS. The Department has demonstrated its commitment to improving its practices and operations. It continued to make progress in FY 2012, but needed to address some concerns to avoid losing momentum and to achieve the reachable goal of a clean opinion in FY 2013. OIG, in turn, will continue to conduct financial statement audits and make recommendations to help DHS meet its challenges and ensure proper stewardship of taxpayer dollars.

Evaluation of DHS' Information Security Program for Fiscal Year 2013

Number: [OIG-14-09](#)

Date: November 21, 2013

Summary: DHS conducted an independent evaluation of its information security program and practices to comply with the requirements of the *Federal Information Security Management Act*. In evaluating progress in implementing its agency-wide information security program, DHS specifically assessed the Department's plans of action and milestones, security authorization processes, and continuous monitoring programs.

DHS continues to improve and strengthen its information security program. During the past year, DHS drafted an ongoing authorization methodology to help improve the security of the Department's information systems through a new risk management approach. This revised approach transitions the Department from a static, paperwork-driven, security authorization process

to a dynamic framework that can provide security-related information on demand to make risk-based decisions based on frequent updates to security plans, security assessment reports, and hardware and software inventories.

Additionally, DHS developed and implemented the *Fiscal Year 2013 Information Security Performance Plan* which defines the performance requirements, priorities, and overall goals for the Department throughout the year. DHS has also taken actions to address the Administration's cybersecurity priorities, which include the implementation of trusted internet connections, continuous monitoring, and strong authentication. While these efforts have resulted in some improvements, components are still not executing all of the Department's policies, procedures, and practices. Our review identified the following more significant exceptions to a strong and effective information security program: (1) systems are being operated without authority to operate; (2) plans of action and milestones are not being created for all known information security weaknesses or mitigated in a timely manner; and (3) baseline security configuration settings are not being implemented for all systems. Additional information security program areas that need improvement include incident detection and analysis, specialized training, account and identity management, and contingency planning. Finally, the Department still needs to consolidate all of its external connections, and complete the implementation of personal identity verification compliant logical access on its information systems and networks.

We are making five recommendations to the Chief Information Security Officer. The Department concurred with all recommendations and has begun to take actions to implement them.

Fiscal Year 2013 Risk Assessment of DHS Charge Card Abuse Prevention Program

Number: [OIG-14-29](#)

Date: January 29, 2014

Summary: The travel, purchase, and fleet charge cards provide the Department of Homeland Security with an efficient mechanism for making small purchases, as well as other numerous benefits. On October 5, 2012, the President signed into law The Government Charge Card Abuse Prevention Act of 2012 (Charge Card Act), Public Law 112-194, which reinforced Administration efforts to prevent waste, fraud, and abuse of Government-wide charge card programs. Under the Charge Card Act, Inspectors General will conduct periodic risk assessments of agency purchase cards (including convenience checks), combined integrated card programs, and travel card programs to analyze the risks of illegal, improper, or erroneous purchases.

DHS has established internal controls and safeguards for purchase, travel, and integrated cards; as well as centrally billed accounts. In most instances, DHS had an adequate framework for internal controls to manage its charge card program. Although the Department has established internal controls for its charge card programs, the Components did not always follow DHS' procedures, and they did not always have procedures in place to supplement those developed by DHS. The Department needs to improve its implementation of internal controls to mitigate the inherent risks associated with the use of charge cards. For example, the Department needs to strengthen its post payment audit process to ensure that Component personnel are complying with appropriate charge card internal controls.

One Component uses the DHS Charge Card Manual as their primary guidance, while others maintain their own guidance and use the DHS manual as an overarching policy. The Department

needs to ensure that the DHS Charge Card Manual and current Components' guidance are consistent and address all Office of Management and Budget regulatory requirements. We assessed the risk that the Department's internal controls over the charge card programs will not prevent illegal, improper, or erroneous purchases.

Based upon the results of our procedures, we determined that there is a moderate level of risk that DHS' internal controls over the charge card programs will not prevent illegal, improper, or erroneous purchases.

The USCG's Oversight of Recommendations from Deepwater Horizon After Action Reports

Number: [OIG-14-42](#)

Date: February 21, 2014

Summary: The USCG did not provide effective oversight of recommendations made to it in Deepwater Horizon (DWH) after action reports, nor could it provide reasonable assurance that corrective actions for the DWH incident addressed the recommendations in these after action reports. The USCG had difficulty tracking the status of specific recommendations contained in after action reports prepared in response to the DWH oil spill. This occurred because management of the process was not fully coordinated and after action report recommendations were not centrally or specifically tracked.

In addition, according to a USCG after action report, the USCG could not be certain that actions resulting from previous oil spills had been implemented, and thus, it encountered some of the same issues in response to the DWH incident. This may have affected the response to the oil spill and could affect the USCG's response to future disasters.

We recommend that the Assistant Commandant for Response Policy:

- 1) Identify or develop a process to ensure that USCG initiatives and subsequent corrective actions, especially those developed as a result of recommendations from DWH after action reports, can be tracked back to individual recommendations.
- 2) Evaluate the use of the Contingency Preparedness System or other USCG systems of record for tracking recommendations and corrective actions from oil spill response after action reports. Consider expanding the use of the identified system of record to all USCG after action reports.

The USCG concurred with both recommendations. It plans to clarify USCG policy for reviewing post-incident reports. The USCG Headquarters office with oversight responsibility for the policy will determine and prioritize which report recommendations the USCG will act on and track these recommendations in the Contingency Preparedness System.

DHS' FY 2013 Compliance with the Improper Payments Elimination and Recovery Act of 2010

Number: [OIG-14-64](#)

Date: April 14, 2014

Summary: To comply with IPERA, an agency is required to conduct risk assessments and report and publish the results of selected program testing in its Annual Financial Report. It must also achieve and report improper payment rates of less than 10 percent for each program. KPMG LLP (KPMG) did not find any instances of noncompliance with IPERA.

Additionally, we reviewed the Department of Homeland Security's processes and procedures for estimating its annual improper payment rates. Based on our review, DHS has made progress in improving its internal controls over the accuracy and completeness of agency reporting and in its efforts to reduce and recapture improper payments. Specifically, no new internal control weaknesses were identified in FY 2013. Also, DHS and the components' efforts in the past year have closed all but one of the open recommendations from the reports— Department of Homeland Security's Compliance with the Improper Payments Elimination and Recovery Act of 2010, OIG-12-48, issued March 2012; and Department of Homeland Security's FY 2012 Compliance with the Improper Payments Elimination and Recovery Act of 2010, OIG-13-47, issued March 2013.

We also determined that the U.S. Customs and Border Protection properly performed IPERA disbursement testing for the Border Security Fencing program.

This report does not contain any new recommendations. However, one recommendation from our report, Department of Homeland Security's FY 2012 Compliance with the Improper Payments Elimination and Recovery Act of 2010, OIG-13-47, March 2013, remains open and resolved.

Preventing Waste, Fraud, Abuse and Mismanagement in Homeland Security – a GAO High-Risk List Review

Number: [Testimony](#)

Date: May 7, 2014

Summary: In its report, *High-risk Series: An Update* (GAO-13-283, February 2013), GAO identified high-risk areas in the Federal government, including areas of particular concern at DHS. This testimony focuses on some high-risk areas that we also identified in our December 2013 report, *Major Management and Performance Challenges Facing the Department of Homeland Security* (OIG-14-17), particularly in managing acquisitions.

Our work has shown that DHS' management of its acquisitions is not as effective and efficient as it could be. This problem stems from three main issues:

- First, DHS' unique mission requires multifaceted and sophisticated acquisitions. Whether acquiring a fleet of helicopters, building a border fence over hundreds of miles of varied terrain, or integrating and managing systems from diverse legacy agencies, DHS' requirements increase the complexity and risk of its acquisitions.
- Second, DHS is working toward a transparent, authoritative governing process — the Acquisition Lifecycle Framework (ALF) — which, if fully implemented, would lead to better oversight and guidance of acquisitions. Unfortunately, DHS components often do not follow this governing process (or any other) in carrying out their acquisitions, and DHS has had difficulty enforcing compliance.
- Third, the components' acquisition decisions often work counter to the Department's stated goal of "One DHS." In planning and managing acquisitions, components often operate in a vacuum; they fail to take into account the needs of other components or they fail to leverage other assets or acquisitions already underway.

We have made recommendations to improve the efficiency and effectiveness of DHS' programs and operations, and DHS has taken some steps to implement our recommendations. However, the

Department continues to struggle with acting as an integrated, single entity to accomplish its mission.

DHS Does Not Adequately Manage or Have Enforcement Authority Over its Components' Vehicle Fleet Operations

Number: [OIG-14-126](#)

Date: August 21, 2014

Summary: Our audit objective was to determine whether, for FY 2012, DHS met requirements to right-size its motor vehicle fleet composition, eliminate underused vehicles, and acquire vehicles that reduce petroleum use and greenhouse gas emissions.

DHS does not adequately manage or have the enforcement authority over its components' fleet operations to ensure that its motor vehicle fleet composition is right-sized. Each DHS component manages its own vehicle fleet, making it difficult for the DHS Fleet Manager to provide adequate oversight and ensure compliance with Federal laws, regulations, policies, and directives. Also, the Department does not have a centralized fleet management information system. For reporting on its motor vehicle fleet inventory, DHS must rely on multiple information systems that contain inaccurate and incomplete vehicle data from the components.

In FY 2012, all of the component vehicle fleets we reviewed included underused vehicles, but DHS did not ensure the components justified retaining the vehicles or removed them from their fleets. In that fiscal year, we estimate that operating these underused vehicles cost between \$35.3 million and \$48.6 million in funds that could have been put to better use.

We recommend that the DHS Under Secretary for Management 1) ensure that the DHS Fleet Manager has adequate oversight and the necessary enforcement authority over component fleet managers' efforts to acquire vehicles, right-size their fleets, and eliminate underused vehicles and 2) implement a single, centralized system of record for the Department's motor vehicle fleet to improve visibility, identify data gaps and inconsistencies, and facilitate collection of vehicle inventory, cost, and usage data.

The Department concurred with our recommendations and provided details on actions being taken to address specific findings and recommendations in the report. According to DHS, CBP, ICE, and NPPD, they have taken several steps since FY 2012 to improve fleet management and ensure fleets are right-sized.

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

This page intentionally left blank.



Homeland
Security



Homeland
Security