Homeland Security

Annual Performance Report

Appendix B: Relevant GAO and OIG Reports

Fiscal Years 2016-2018

With honor and integrity, we will safeguard the American people, our homeland, and our values.

We are DHS

About this Report

The *U.S. Department of Homeland Security Annual Performance Report for Fiscal Years (FY) 2016-2018* presents the Department's performance measures and applicable results aligned to our missions, provides the planned performance targets for FY 2017 and FY 2018, and includes information on the Department's Strategic Review and our Agency Priority Goals. In addition, this report presents several FY 2016 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 2016 – 2018 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 15, 2016.
- ***DHS Annual Performance Report***: Delivery date – May 22, 2017
- ***DHS Summary of Performance and Financial Information:*** Delivery date – March 29, 2017.

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

For more information, contact:

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

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

Homeland Security

Visit Our Website
www.dhs.gov

Table of Contents

Introduction

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

This appendix provides, in tabular format, a list of the more significant DHS program evaluations conducted in FY 2016 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 2015 DHS OIG reports is available at: https://www.oig.dhs.gov/index.php?option=com_content&view=article&id=222&Itemid=69.

Mission 1: Prevent Terrorism and Enhance Security

Goal 1.1: Prevent Terrorist Attacks

GAO Reports

TSA Is Taking Steps to Improve Expedited Screening Effectiveness, but Improvements in Screener Oversight Are Needed

Number: GAO-16-707T
Date: 06/07/2016
Summary: The Transportation Security Administration (TSA) has taken steps intended to improve the security effectiveness of expedited passenger screening since GAO reported on it in December 2014. These steps include:

- Adjusting the TSA Pre✓® Risk Assessment program algorithm used to assign passengers scores and identify low risk passengers;
- Limiting the use of Managed Inclusion to airports that employ canine teams to detect explosives; and,
- Developing plans to test the security effectiveness of the Managed Inclusion process as an overall system–ensuring that the testing adheres to established design practices.

According to a TSA memorandum dated November 2015, TSA made changes to TSA Pre✓® Risk Assessment program and Managed Inclusion process as a result of the findings and recommendations included in three prior Department of Homeland Security Office of Inspector General audit reports. According to TSA, these changes were necessary to ensure security and resulted in a 20 percent decrease in the number of individuals receiving expedited screening. Previously, in December 2014, GAO found that TSA had not tested the overall effectiveness of the Managed Inclusion process, and recommended that TSA ensure that its planned testing adhere to established evaluation design practices to yield reliable test results. DHS concurred with the recommendation and plans to begin testing the effectiveness of the Managed Inclusion process as a system during fiscal year 2016.

TSA uses data on Transportation Security Officer (TSO) performance obtained from its various testing programs to ensure that individual TSOs are (1) demonstrating through annual proficiency reviews and resulting recertification that they are qualified to continue conducting passenger and checked baggage screening, and (2) demonstrating proficiency during live screening operations in adhering to screening procedures. However, in a report containing sensitive security information completed in May 2016, GAO found that TSA's ability to fully evaluate TSO performance in screening passengers and baggage for prohibited items is constrained by incomplete and unreliable testing data and a lack of data analysis. For example, some airports did not report testing data on

TSOs' ability to identify prohibited items over fiscal years 2009 through 2014 as required by TSA policy. TSA officials also stated they do not systematically analyze test results to determine any national trends for informing future TSO training. In addition, TSA determined that pass rate data for one of its covert testing programs that uses role players at airports to assess TSO performance was unreliable. Specifically, testing by an independent contractor indicated that TSA's covert testing data likely overstated TSO performance. TSA is taking action to determine the root cause of the variance in the testing results and is implementing corrective actions. Further, GAO found that TSA does not track the implementation, where appropriate, of recommendations made based on the covert testing results. DHS concurred with GAO's recommendations made in its May 2016 report and is planning actions to address them.

In its May 2016 report, GAO recommended that TSA ensure that (1) airports submit complete TSO performance data, (2) the data are analyzed nationally, and (3) implementation of covert testing recommendations are tracked. DHS concurred and is taking actions to address the recommendations.

Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates

Number: GAO-16-632
Date: 05/31/2016
Summary: This is a public version of a sensitive report that GAO issued in March 2016. Information that TSA deems "Sensitive Security Information" has been removed.

The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) has made progress in assessing the threat, vulnerability, and consequence components of risk to airport perimeter and access control security (airport security) since GAO last reported on the topic in 2009, such as developing its Comprehensive Risk Assessment of Perimeter and Access Control Security (Risk Assessment of Airport Security) in May 2013. However, TSA has not updated this assessment to reflect changes in the airport security risk environment, such as TSA's subsequent determination of risk from the insider threat—the potential of rogue aviation workers exploiting their credentials, access, and knowledge of security procedures throughout the airport for personal gain or to inflict damage. Updating the Risk Assessment of Airport Security with information that reflects this current threat, among other things, would better ensure that TSA bases its risk management decisions on current information and focuses its limited resources on the highest-priority risks to airport security. Further, TSA has not comprehensively assessed the vulnerability—one of the three components of risk—of TSA-regulated (i.e., commercial) airports system-wide through its joint vulnerability assessment (JVA) process, which it conducts with the Federal Bureau of Investigation (FBI), or another process. From fiscal years 2009 through 2015, TSA conducted JVAs at 81 (about 19 percent) of the 437 commercial airports nationwide. TSA officials stated that they have not conducted JVAs at all airports system-wide because of resource constraints. While conducting JVAs at all commercial airports may not be feasible given budget and resource constraints, other approaches, such as providing all commercial airports with a self-vulnerability assessment tool, may allow TSA to assess vulnerability at airports system-wide.

Since 2009, TSA has taken various actions to oversee and facilitate airport security; however, it has not updated its national strategy for airport security to reflect changes in its Risk Assessment of

Airport Security and other security-related actions. TSA has taken various steps to oversee and facilitate airport security by, among other things, developing strategic goals, and evaluating risks. For example, in 2012 TSA developed its National Strategy for Airport Perimeter and Access Control Security (Strategy), which defines how TSA seeks to secure the perimeters and security-restricted areas of the nation's commercial airports. However, TSA has not updated its Strategy to reflect actions it has subsequently taken, including results of the 2013 Risk Assessment and new and enhanced security activities, among other things. Updating the Strategy to reflect changes in the airport security risk environment and new and enhanced activities TSA has taken to facilitate airport security would help TSA to better inform management decisions and focus resources on the highest-priority risks, consistent with its strategic goals.

GAO is making six recommendations, including that TSA update its Risk Assessment of Airport Security, develop and implement a method for conducting a system-wide assessment of airport vulnerability, and update its National Strategy for Airport Perimeter and Access Control Security DHS concurred with the recommendations and identified planned actions to address the recommendations.

Transportation Security: TSA Has Taken Actions to Address Transportation Security Acquisition Reform Act Requirements

Number: GAO-16-285
Date: 02/17/2016
Summary: The Transportation Security Administration (TSA) in the Department of Homeland Security (DHS) has policies and procedures that generally address requirements of the December 2014 Transportation Security Acquisition Reform Act (TSARA). Specifically, TSA policy and procedures address TSARA requirements for justifying acquisitions, establishing baselines, managing inventory, and submitting plans, among other requirements.

Justifying Acquisitions: TSA had taken action toward addressing most TSARA requirements related to justifying acquisitions prior to TSARA's enactment because they were required by existing DHS and TSA acquisition policies. Consistent with TSARA, TSA amended its policies to notify Congress within 30 days of awarding contracts exceeding $30 million for the acquisition of security-related technology. According to agency officials, TSA has not made any such new acquisitions since the enactment of TSARA.

Acquisition Baselines: TSA policies require that it prepare an acquisition program baseline, risk management plan, and staffing requirements before acquiring security-related technology. Consistent with TSARA, TSA established policies to notify Congress within 30 days of making a finding of performance failures, schedule delays, or cost overruns constituting a breach against acquisition program baselines. TSA reported that it had not experienced breaches in any existing acquisitions (i.e., those in place prior to December 2014) since the enactment of TSARA.

Managing Inventory: TSA's policies and procedures address TSARA requirements for using existing units before procuring more equipment; tracking the location, use, and quantity of security-related equipment in inventory; and using just-in-time delivery to avoid warehousing equipment.

Submitting Plans: TSA submitted its Technology Investment Plan and Small Business Report to Congress as required by TSARA. The Technology Investment Plan addresses required elements such as identifying security gaps and security-related technology needs and processes. The Small Business Report includes an action plan for integrating the concerns of small businesses into acquisition processes and increasing outreach to targeted small businesses.

DHS and TSA officials said that TSA has not yet identified any efficiencies, cost savings, or delays from its implementation of TSARA. They added that because many of the policies and procedures that meet the provisions of the act were in place prior to the enactment of TSARA, it was unlikely for TSARA to result in major efficiencies, cost savings, or delays. According to TSA officials, TSA has developed mechanisms to monitor various aspects of TSARA, such as tracking progress in implementing planned technology programs.

TSA Acquisitions: Further Actions Needed to Improve Efficiency of Screening Technology Test and Evaluation

Number: GAO-16-117
Date: 02/17/2016
Summary: The Transportation Security Administration's (TSA) test and evaluation process has enabled TSA and Department of Homeland Security (DHS) officials to identify passenger and baggage screening technologies that will meet mission needs, but technology failures during testing have contributed to inefficiencies in the acquisition process. Consistent with departmental guidance and acquisition best practices, TSA's test and evaluation process provides information regarding the ability of technologies to meet mission needs before agency officials decide whether to begin full production, saving the agency from investing in potentially expensive yet ineffective equipment. From June 2010 to July 2015, half of the 22 systems that TSA tested successfully completed qualification and operational testing. TSA procured all but 1 of the 11 successful systems. Technologies that entered the test and evaluation process and were immature required significant modifications and retesting.

TSA has taken steps to improve its test and evaluation process by helping ensure technologies are mature before entering testing, but it is too soon to tell whether these actions will address all of the factors that contribute to acquisition inefficiencies. A key action TSA is taking involves developing a third party testing strategy, through which a third party will help ensure systems are mature prior to entering TSA's test and evaluation process. TSA plans to implement its approach in 2016, but it has yet to finalize key aspects of the strategy. For example, TSA has not identified whether there are a sufficient number of eligible third party testers or established a mechanism to oversee that testing. Without a finalized strategy, TSA risks unintended consequences, such as increasing acquisition costs. Further, TSA has not conducted or documented a comprehensive assessment of testing data and thus may be missing opportunities to identify additional areas for improvements to its acquisition process. An assessment of this data, such as costs incurred, could help TSA guide future reforms to the test and evaluation process to help ensure they address factors contributing to any acquisition inefficiencies.

DHS OIG Reports

Transportation Security Administration Needs a Crosscutting Risk-Based Security Strategy

Number: OIG-16-134
Date: 09/09/2016
Summary: TSA is charged with securing the Nation's transportation systems — highway, freight rail, aviation, mass transit, and pipeline — to ensure freedom of movement for people and commerce. TSA directly manages security programs such as passenger and baggage screening for the aviation mode, but its primary role for surface (non-aviation) modes is oversight and regulation. Since 2011, TSA has publicized that it uses an "intelligence-driven, risk-based approach" across all transportation modes.

We determined that TSA lacks an intelligence-driven, risk-based security strategy that informs security and resource decisions across all transportation modes. TSA's publicized "intelligence driven, risk-based approach" was designed for the aviation mode and chiefly for air passenger screening. Though TSA has security programs for the surface modes, its agency-wide risk management organizations provide little oversight of these programs. In addition, TSA lacks a formal process to incorporate risk in its budget formulation decisions. A crosscutting risk-based security strategy would help ensure all transportation modes consistently implement risk-based security and help decision makers align resources effectively. TSA concurred with our recommendations.

TWIC Background Checks are Not as Reliable as They Could Be

Number: OIG-16-128
Date: 09/01/2016
Summary: TSA's leadership, responsible for issuing Transportation Worker Identification Credentials (TWIC), does not provide sufficient oversight and guidance to ensure that the TWIC program operates effectively. Specifically, within the background check process, which TSA calls the security threat assessment:

- Fraud detection techniques are not monitored and used in completing the background check;
- Adjudicators may grant TWICs even if questionable circumstances exist;
- Key quality assurance and internal control procedures are missing from the background check and terrorism vetting processes; and
- New efforts tested for continuous vetting for disqualifying criminal or immigration offenses lack measures to determine the best solution.

These issues exist, in part, because TSA leadership relies on the TWIC program office to implement necessary improvements; however, the TWIC program office focuses more on customer service than effectiveness of the program. Additionally, because of TSA's organizational structure, the TWIC program office lacks visibility into and authority over the other offices within TSA that support the TWIC program. As a result, there is a risk that someone with major criminal or

immigration offenses maintains access to secured areas of maritime facilities. TSA concurred with the recommendations.

Verification Review of Transportation Security Administration's Screening of Passengers by Observation Techniques/Behavior Detection and Analysis Program

Number: OIG-16-111-VR
Date: 07/08/2016
Summary: In 2013, we audited TSA's then-Screening of Passengers by Observation Techniques (SPOT) program. TSA has since changed the name of the program from the SPOT program to the BDA program. The intent of the program is to screen passengers by observing their behavior in order to detect potential high-risk travelers. The program uses Behavior Detection Officers (BDO) to detect passenger behaviors that may be indicative of stress, fear, or deception. Currently, TSA operates the program at 87 airports (BDA airports) with 2,660 full-time staff. Between fiscal years 2007 and 2015, the program expended an estimated $1.5 billion.

Our 2013 audit reported that TSA had not implemented a comprehensive strategic plan to ensure the SPOT program's success and did not have adequate controls to ensure the completeness, accuracy, authorization, and validity of program data. To address the 2013 report's recommendations, TSA implemented a comprehensive strategic plan and addressed the accuracy and reliability of data by conducting a large scale data audit to identify and correct errors in its referral data.1 TSA also implemented additional controls to improve the timeliness and accuracy of recorded referrals. Subsequently, we closed the recommendations because we determined that TSA's corrective actions met the intent of our recommendations.

In this verification review, we evaluated whether TSA's on-going actions still meet the intent of these recommendations. We did not look at the program's effectiveness, as this review is limited in scope. We intend to conduct an audit of the program's effectiveness in FY 2017.

Verification Review Results: TSA created a comprehensive strategic plan and developed controls to assure completeness, accuracy, authorization, and validity of Performance Measurement Information System referral data. These actions were sufficient to close the two selected recommendations. However, TSA has not yet executed all the actions described in its plans to demonstrate the program's effectiveness. Since we closed our recommendations in March 2014, TSA updated and revised its strategic plan for fiscal years 2016 through 2018, and it incorporated newly developed performance metrics. As of May 2016, TSA reported it implemented these new performance metrics at all 87 BDA airports, but TSA has yet to fully assess them to determine their effectiveness.

Furthermore, TSA has not fully transitioned to a new reporting system that is designed to improve data deficiencies in the Performance Measurement and Information System. Therefore, we were unable to fully assess whether TSA's corrective actions for these two recommendations will further improve BDA performance and reporting.

December 3, 2015 – San Bernardino Incident

Number: No Number Provided
Date: 06/01/2016
Summary: On March 16, 2016, Senator Ron Johnson, Chairman of the Homeland Security and Government Affairs Committee (HSGAC), requested that the Office of Inspector General review the events that took place at the U.S. Citizenship and Immigration Services (USCIS), San Bernardino, California, office on December 3, 2015. Our objective was: 1) to conduct a factual inquiry into the incident and 2) to determine if Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) was attempting to identify and retaliate against an employee who originally reported information to the Senate. We have substantially completed our review.

We concluded that the USCIS Field Office Director at the San Bernardino office improperly delayed HSI agents from conducting a lawful and routine law enforcement action, but when the Field Office Director elevated the situation to her supervisors, the situation was corrected. We found that the contract security personnel improperly prevented HSI personnel from entering the building. Finally, we found that there was no attempt by ICE leadership or supervisory personnel within HSI to attempt to retaliate against the individuals who notified HSGAC of the situation. We have also concluded that the Field Office Director was not candid with OIG investigators during her interview.

We conducted this investigation from March 17, 2016 until April 8, 2016. We conducted approximately 23 interviews, reviewed HSI and USCIS policies, researched HSI authority to enter government buildings and conduct arrests, and obtained email, text, and phone records.

TSA Oversight of National Passenger Rail System Security

Number: OIG-16-91
Date: 05/13/2016
Summary: TSA has limited regulatory oversight processes to strengthen passenger security at Amtrak because the component has not fully implemented all requirements from the 9/11 Act. Federal regulations require Amtrak to appoint a rail security coordinator, report significant security concerns to TSA, and to allow TSA to conduct inspections. The 9/11 Act requires TSA to establish additional passenger rail regulations; however, the component has not fully implemented them. Specifically, TSA has not issued regulations to assign rail carriers to high-risk tiers; established a rail training program; and conducted security background checks of frontline rail employees. In the absence of formal regulations, TSA relies on outreach programs, voluntary initiatives, and recommended measures to assess and improve rail security for Amtrak.

TSA attributes the delays in implementing the rail security requirements from the 9/11 Act primarily to the complex Federal rulemaking process. Although the rulemaking process can be lengthy, TSA has not urgently prioritized the need to implement these rail security requirements. This is evident from TSA's inability to satisfy these requirements more than 8 years after the legislation was passed. Without fully implementing and enforcing the requirements from the 9/11 Act, TSA's ability to strengthen passenger rail security may be diminished. The absence of

regulations also impacts TSA's ability to require Amtrak to make security improvements that may prevent or deter acts of terrorism.

IT Management Challenges Continue in TSA's Security Technology Integrated Program (Redacted)

Number: OIG-16-87
Date: 05/10/2016
Summary: As described in our prior reports on this issue, numerous deficiencies continue in STIP IT security controls, including unpatched software and inadequate contractor oversight. This occurred because TSA typically has not managed STIP equipment in compliance with departmental guidelines regarding sensitive IT systems. Failure to comply with these guidelines increases the risk that baggage screening equipment will not operate as intended, resulting in potential loss of confidentiality, integrity, and availability of TSA's automated explosive, passenger, and baggage screening programs.

TSA did not effectively manage all IT components of STIP as IT investments. Based on senior-level TSA guidance, TSA officials did not designate these assets as IT equipment. As such, TSA did not ensure that IT security requirements were included in STIP procurement contracts, which promoted the use of unsupported operating systems that created security concerns and forced TSA to disconnect STIP TSE from the network. TSA also did not report all STIP IT costs in its annual budgets, hindering the agency from effectively managing and evaluating the benefits and costs of STIP.

Recently, TSA has taken steps to resolve these STIP deficiencies. For example, according to a TSA staff member, system owners may no longer prevent the implementation of required software patches. TSA is also working to include cybersecurity requirements in the procurement process. However, more time is needed to determine the effectiveness of these improvement initiatives. The agency concurred with all 11 recommendations. All recommendations are resolved and open, except for recommendation 5, which is unresolved and open.

TSA's Human Capital Services Contract Terms and Oversight Need Strengthening

Number: OIG-16-32
Date: 01/29/2016
Summary: Although TSA ensures the contractor meets the terms and conditions of the human capital services contract, its oversight could be more effective. Specifically, TSA has limited options for holding the contractor accountable for performance deficiencies. There were instances in which TSA did not hold the contractor monetarily accountable for personally identifiable information violations. TSA also did not hold the contractor monetarily liable for noncompliance with statement of work requirements relating to veterans' preference.

Additionally, TSA needs to improve its assessment and monitoring of contractor performance. Performance metrics are not comprehensive. TSA inflates performance evaluation scores and those scores are not consistently affected by poor performance. Furthermore, TSA does not consistently

conduct day-to-day independent monitoring of contractor performance. TSA's weak contract oversight resulted in performance awards that do not accurately reflect performance. In addition, award fees, totaling $4.5 million, may not be justified, and TSA has no assurance it received the best value for its money. TSA concurred with all five recommendations. We consider one recommendation resolved and closed and two recommendations resolved and open. However, for two recommendations, TSA needs to identify additional steps to address

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: Improvements Needed for DHS's Chemical Facility Whistleblower Report Process

Number: GAO-16-572
Date: 07/12/2016
Summary: Of the 105 reports that the Department of Homeland Security (DHS) received under its interim process for whistleblowers from June 16, 2015 (the date DHS was mandated to begin collecting reports by), to April 19, 2016, DHS closed 97 because they did not pertain to Chemical Facility Anti-Terrorism Standards (CFATS) regulations, and referred 70 of the 97 to other federal agencies with legal authority relevant to the reports. DHS determined that 8 of the 105 reports involved potential CFATS violations, and after further review, that 1 report involved an actual CFATS violation. As a result of this report, DHS required the chemical facility to register with DHS as a CFATS-regulated facility.

In June 2015, DHS implemented an interim process to respond to whistleblower reports involving CFATS and has followed its process since then; however, DHS does not have a documented process and procedures to investigate whistleblower retaliation reports. The Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (CFATS Act of 2014) prohibits retaliation against whistleblowers. According to DHS, the department has not received a report of whistleblower retaliation that it substantiated since implementing the interim process and any future retaliation reports would be addressed on a case-by-case basis. However, without a documented process and procedures for investigating whistleblower retaliation reports, DHS may not be able to effectively and efficiently investigate any future retaliation reports. In addition, DHS maintains a telephone tip line and a website with an e-mail address to receive CFATS whistleblower reports. However, the tip line greeting provides no guidance and the website provides limited guidance about the type of information that would be most useful to DHS for addressing the reports. GAO's analysis of 105 reports received by DHS from June 16, 2015, to April 19, 2016, identified challenges that DHS experienced in vetting reports due to insufficient information, such as the name

or location of the chemical facility. Additional guidance explaining the detailed information that DHS needs to review reports could help reduce the amount of follow-up time to obtain this information. GAO recommends that DHS develop a documented process and procedures to address whistleblower retaliation reports, and provide additional guidance on the DHS whistleblower website and telephone tip line. DHS agreed with GAO's recommendations.

Combating Nuclear Smuggling: NNSA's Detection and Deterrence Program Is Addressing Challenges but Should Improve Its Program Plan

Number: GAO-16-460
Date: 06/17/2016
Summary: International nuclear and radiological smuggling threatens national security. According to the Department of Homeland Security, detecting and interdicting these materials as far away from the United States as possible increases the probability of successfully deterring nuclear and radiological smuggling into the United States. To help interdict these materials, NNSA's NSDD program has partnered with 59 countries to provide radiation detection equipment and support. GAO was asked to review key aspects of the NSDD program.

The National Nuclear Security Administration's (NNSA) Nuclear Smuggling Detection and Deterrence (NSDD) program has developed a program plan that includes four 5-year goals to guide its efforts; however, NSDD cannot measure its progress toward completing key activities and achieving these goals because its program plan does not fully incorporate leading practices for program management. Leading practices include having measurable outcome-oriented goals, goals for all key activities, performance measures that align with these goals, and details for how and when key activities will be completed and goals achieved. However, NSDD's goals are not all measurable, some describe actions rather than outcomes, and they do not fully address all of the program's key activities. In addition, its performance measures are not aligned with these goals, and its program plan does not detail how it will complete key program activities or achieve its goals. Absent a program plan incorporating these leading practices, NSDD may not be able to determine when it has accomplished its mission and risks continuing to deploy equipment past the point of diminishing returns.

In each of the three selected partner countries GAO visited—Azerbaijan, Bulgaria, and Georgia—law enforcement officers and government officials attributed multiple cases of successful detection, deterrence, and interdiction of smuggled nuclear and radiological materials to the use of NSDD-provided radiation detection equipment. For example, one of these countries has been involved with 21 such smuggling cases over the past 10 years, with over 50 convictions made as a result. Moreover, some cases in these countries have involved the detection and interdiction of highly enriched uranium, which can be used to develop a nuclear weapon.

NSDD faces an unusual set of challenges in performing its work, many largely outside of its control. Nonetheless, the program is taking actions to mitigate the effects of these challenges. For example, NSDD officials cited changing conditions in partner countries as a key challenge. In particular, NSDD officials noted that the conflict between the Ukrainian government and separatist groups that began in 2014 has led to the destruction of 29 radiation portal monitors, and NSDD

officials do not know whether the program will be able to fix or replace them and, if so, when. To mitigate this challenge, NSDD plans to deploy additional radiation detection equipment at key locations outside the conflict area.

Biosurveillance: Ongoing Challenges and Future Considerations for DHS Biosurveillance Efforts

Number: GAO-16-413T
Date: 02/11/2016
Summary: Since 2009, GAO has reported on progress and challenges with two of the Department of Homeland Security's (DHS) biosurveillance efforts—the National Biosurveillance Integration Center (NBIC) and the BioWatch program (designed to provide early detection of an aerosolized biological attack). In December 2009, GAO reported that NBIC was not fully equipped to carry out its mission because it lacked key resources—data and personnel—from its partner agencies, which may have been at least partially the result of collaboration challenges it faced. For example, some partners reported that they did not trust NBIC to use their information and resources appropriately, while others were not convinced of the value that working with NBIC provided because NBIC's mission was not clearly articulated. GAO recommended that NBIC develop a strategy for addressing barriers to collaboration and develop accountability mechanisms to monitor these efforts. DHS agreed, and in August 2012, NBIC issued the NBIC Strategic Plan, which is intended to provide NBIC's strategic vision, clarify the center's mission and purpose, and articulate the value that NBIC seeks to provide to its partners, among other things. In September 2015, GAO reported that despite NBIC's efforts to collaborate with interagency partners to create and issue a strategic plan that would clarify its mission and the various efforts to fulfill its three roles—analyzer, coordinator, and innovator—a variety of challenges remained when GAO surveyed NBIC's interagency partners in 2015. Notably, many of these partners continued to express uncertainty about the value NBIC provided. GAO identified options for policy or structural changes that could help NBIC better fulfill its biosurveillance integration mission, such as changes to NBIC's roles.

Since 2012, GAO has reported that DHS has faced challenges in clearly justifying the need for the BioWatch program and its ability to reliably address that need (to detect attacks). In September 2012, GAO found that DHS approved a next-generation BioWatch acquisition in October 2009 without fully developing knowledge that would help ensure sound investment decision making and pursuit of optimal solutions. GAO recommended that before continuing the acquisition, DHS reevaluate the mission need and possible alternatives based on cost-benefit and risk information. DHS concurred and in April 2014, canceled the acquisition because an alternatives analysis did not confirm an overwhelming benefit to justify the cost. Having canceled the next generation acquisition, DHS continues to rely on the currently deployed BioWatch system for early detection of an aerosolized biological attack. However, in 2015, GAO found that DHS lacks reliable information about the current system's technical capabilities to detect a biological attack, in part because in the 12 years since BioWatch's initial deployment, DHS has not developed technical performance requirements for the system. GAO reported in September 2015 that DHS commissioned tests of the current system's technical performance characteristics, but without performance requirements, DHS cannot interpret the test results and draw conclusions about the system's ability to detect attacks. DHS is considering upgrades to the current system, but GAO recommended that DHS not pursue upgrades until it establishes technical performance requirements

to meet a clearly defined operational objective and assesses the system against these performance requirements. DHS concurred and is working to address the recommendation.

Biodefense: The Nation Faces Multiple Challenges in Building and Maintaining Biodefense and Biosurveillance

Number: GAO-16-547T
Date: 04/14/2016
Summary: The biodefense enterprise is fragmented and does not have strategic oversight to promote efficiency and accountability. Specifically, the biodefense enterprise lacks institutionalized leadership enterprise-wide to provide strategic oversight and coordination. In 2011, GAO reported, there are more than two dozen presidentially appointed individuals with biodefense responsibilities and numerous federal agencies with mission responsibilities for supporting biodefense activities, but no individual or entity with responsibility for overseeing the entire biodefense enterprise. In 2011, GAO reported that the Homeland Security Council (HSC) should consider establishing a focal point for federal biodefense coordination. In December 2014, National Security Council (NSC) staff, which supports the HSC, told GAO that two of its directorates work together as the focal point for federal biodefense efforts. This is an important step in promoting a comprehensive and coordinated approach to biodefense, but strategic leadership issues persist. In October 2015, a report by the Blue Ribbon Study Panel on Biodefense stated strategic leadership issues persist and called for a focal point to provide strategic leadership, noting that elevating authority above the agency-level can help overcome the challenges faced by the biodefense enterprise. The Study Panel found that White House councils and offices generally only become involved when a specific biodefense issue affects a prominent ongoing responsibility—a method which is not consistent with our call for a strategic approach.

In 2011, GAO also reported that while some high-level biodefense strategies have been developed, there is no broad, integrated national strategy that encompasses all stakeholders with biodefense responsibilities that can be used to guide the systematic identification of risk; assess resources needed to address those risks; and prioritize and allocate investment across the entire biodefense enterprise. GAO reported that the overarching biodefense enterprise would benefit from strategic oversight mechanisms, including a national strategy, to help ensure efficient, effective, and accountable results, and suggested the HSC take action. However, as of February 2016, such a strategy had not been developed.

Biosurveillance, an aspect of biodefense, also faces key challenges at all levels of government that transcend what any one agency can address on its own, and our more recent and ongoing work continues to highlight these challenges. In 2010, GAO recommended the HSC establish a focal point to lead the development of a national biosurveillance strategy that clarifies roles and responsibilities, provides goals and performance measures, and identifies resource and investment needs, among other elements. However, the recommendations have not been fully implemented. Since 2009 GAO's has also identified challenges with specific biosurveillance capabilities. Specifically, GAO has identified biosurveillance capability challenges with, among other topics, (1) state and local public heath capabilities, (2) animal health surveillance capabilities, and (3) two Department of Homeland Security biosurveillance efforts—the National Biosurveillance Integration Center (NBIC) and the BioWatch Program (which aims to provide early indication of an aerosolized biological weapon attack). However, not all recommendations have been implemented.

Biosurveillance: DHS Should Not Pursue BioWatch Upgrades or Enhancements Until System Capabilities Are Established

Number: GAO-16-99
Date: 10/23/2015
Summary: The Department of Homeland Security (DHS) lacks reliable information about BioWatch Gen-2's technical capabilities to detect a biological attack and therefore lacks the basis for informed cost-benefit decisions about upgrades to the system. DHS commissioned several tests of the technical performance characteristics of the current BioWatch Gen-2 system, but has not developed performance requirements that would enable it to interpret the test results and draw conclusions about the system's ability to detect attacks. Although DHS officials said that the system can detect catastrophic attacks, which they define as attacks large enough to cause 10,000 casualties, they have not specified the performance requirements necessary to reliably meet this operational objective. In the absence of performance requirements, DHS officials said computer modeling and simulation studies support their assertion. However, none of these studies were designed to incorporate test results from the Gen-2 system and comprehensively assess the system against the stated operational objective. Additionally, DHS has not prepared an analysis that combines the modeling and simulation studies with the specific Gen-2 test results to assess the system's capabilities to detect attacks. Finally, we found limitations and uncertainties in the four key tests of the Gen-2 system's performance. Because it is not possible to test the BioWatch system directly by releasing live biothreat agents into the air in operational environments, DHS relied on chamber testing and the use of simulated biothreat agents, which limit the applicability of the results. These limitations underscore the need for a full accounting of statistical and other uncertainties, without which decision makers lack a full understanding of the Gen-2 system's capability to detect attacks of defined types and sizes and cannot make informed decisions about the value of proposed upgrades.

The actions and decisions DHS made regarding the acquisition and testing of a proposed next generation of BioWatch (Gen-3) partially aligned with best practices GAO previously identified for developmental testing of threat detection systems. For example, best practices indicate that resilience testing, or testing for vulnerabilities, can help uncover problems early. While DHS took steps to help build resilience into the Gen-3 testing, future testing could be improved by using more rigorous methods to help predict performance in different operational environments. DHS canceled the Gen-3 acquisition in April 2014, but GAO identified lessons DHS could learn by applying these best practices to the proposed Gen-2 upgrades.

According to experts and practitioners, the polymerase chain reaction (PCR), which detects genetic signatures of biothreat agents, is the most mature technology to use for an autonomous detection system. DHS is considering autonomous detection as an upgrade to Gen-2, because according to DHS, it may provide benefits such as reduction in casualties or clean-up costs. But the extent of these benefits is uncertain because of several assumptions, such as the speed of response after a detection, that are largely outside of DHS's control. As a result, the effectiveness of the response—and the number of lives that could be saved—is uncertain. Further, an autonomous detection system must address several likely challenges, including minimizing possible false positive readings, meeting sensitivity requirements, and securing information technology networks. GAO recommends DHS not pursue upgrades or enhancements for Gen-2 until it reliably establishes

the system's current capabilities. GAO also recommends DHS incorporate best practices for testing in conducting any system upgrades. DHS generally concurred with GAO's recommendations.

Combating Nuclear Smuggling: Risk-Informed Covert Assessments and Oversight of Corrective Actions Could Strengthen Capabilities at the Border

Number: GAO-16-191T
Date: 10/25/2015
Summary: In its September 2014 report, GAO reported that the Department of Homeland Security (DHS) U.S. Customs and Border Protection's (CBP) Operational Field Testing Division (OFTD) conducted 144 covert operations at 86 locations from fiscal years 2006 through 2013. OFTD selected these locations from a total of 655 U.S. air, land, and sea port facilities; checkpoints; and certain international locations. The results of these operations showed differences in the rates of success for interdicting smuggled nuclear and radiological materials across facility types. OFTD officials stated that the results of its covert operations could be used to assess capabilities at the individual locations tested; but not across all U.S. ports of entry and permanent checkpoints.

GAO also reported that CBP had not conducted a risk assessment to inform and prioritize factors, such as locations, and types of nuclear materials and technologies to be tested in covert operations. CBP had a $1 million budget for covert operations of various activities—including nuclear and radiological testing—from fiscal years 2009 through 2013. Given limited resources, assessing risk to prioritize the most dangerous materials, most vulnerable locations, and most critical equipment for testing through covert operations, could help DHS inform its decisions on how to use its limited resources effectively. DHS agreed with GAO's recommendation to use a risk assessment to inform priorities for covert test operations, but the recommendation remains open. As of October 2015, CBP officials stated that they developed a threat matrix to help determine the sea ports of entry at the highest risk of nuclear and radiological smuggling, but had not completed its assessments for air and land ports of entry.

Finally, GAO reported that OFTD had not issued reports annually as planned on covert operation results and recommendations, which limited CBP oversight for improving capabilities to detect and interdict smuggling at the border. At the time, OFTD had issued three reports on the results of its covert operations at U.S. ports of entry since 2007. However, OFTD officials stated that because of resource constraints, reports had not been timely and did not include the results of covert tests conducted at checkpoints. GAO further reported that OFTD tracked the status of corrective actions taken in response to findings in these reports, but did not track corrective actions identified from their individual covert operations that were not included in these reports. Establishing appropriate time frames and addressing barriers for reporting covert operations results, and developing a mechanism to track all corrective actions would help enhance CBP's accountability for its covert testing and could help inform CBP about further equipment or training required to protect U.S. borders. DHS agreed with GAO recommendations to determine timeframes and address barriers for reporting results, and to track corrective actions; stating that it would address them by April 2015 and December 2014, respectively. As of October 2015, these recommendations remain open as CBP works to fully implement or document actions taken. CBP officials stated they have issued a standard operating procedure containing reporting timeframes, but have not finalized a directive to

address this recommendation. GAO is awaiting documentation to demonstrate that CBP is using the database it developed for tracking corrective actions.

GAO previously recommended DHS use a risk assessment to inform priorities for covert test operations, determine time frames and address barriers for reporting results, and track corrective actions. DHS concurred with the recommendations and reported actions underway to address them. GAO is not making any new recommendations in this testimony.

DHS OIG Reports

No OIG reports were available that aligned to this goal.

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

GAO Reports

U.S. Secret Service: Data Analyses Could Better Inform the Domestic Field Office Structure

Number: GAO-16-288
Date: 2/10/2016
Summary: This is a public version of a sensitive report that GAO issued in November 2015. Information that the Secret Service deemed sensitive has been removed.

From fiscal years 2009 through 2014, the annual cost of the U.S. Secret Service's domestic field office structure—including 115 field offices, resident offices, and resident agencies—ranged from $500 million to $549 million, but the Secret Service did not accurately record cost data for some offices. GAO determined that although the Secret Service's cost data were reasonably reliable in the aggregate, salary and benefit costs may not have been accurately recorded in the agency's time and attendance system for 21 of 73 of the agency's smaller offices. Specifically,

- thirteen resident offices and resident agencies likely had their salaries and benefits costs attributed to the field offices in their districts, and
- eight had higher than expected salaries and benefits costs that may include the salaries and benefits of personnel in field offices.

By implementing a review process to ensure time and attendance charge codes for cost data are correctly established, the Secret Service could reliably determine the cost of each of its domestic offices.

The Secret Service's domestic offices predominately carry out the agency's investigative mission of various financial and electronic crimes and play an integral role in providing protection. GAO's analysis of Secret Service data from fiscal years 2009 through 2014 found that domestic offices removed at least $18 million in counterfeit funds from circulation annually, and coordinated with state and local partners to support between 5,597 and 6,386 protective visits each year. The Secret Service has developed a performance system, which aligns with its missions, to assess domestic office contributions to the agency's missions, which vary by office.

GAO also found that the Secret Service uses data to adjust staffing for the domestic offices, but the agency does not fully use all available data to analyze its domestic field office structure. For example, the Secret Service has not compared domestic field office districts' costs relative to performance or used personnel travel data to analyze whether the domestic offices are optimally located and sized to best meet the agency's mission needs. GAO's analyses of cost, performance, and travel data indicated that some field office districts were more efficient than others and personnel from four domestic offices frequently traveled to non-Secret Service office locations for investigations, potentially indicating the need for a Secret Service presence in these locations. This type of analysis could help the Secret Service determine if its field office structure is responsive to changing conditions and if an adjustment to the structure is warranted. By conducting an analysis of its domestic offices using cost and performance data, among other data as appropriate, the Secret Service could be better positioned to ensure that its domestic field office structure is meeting its mission needs.

GAO recommends, among other things, that the Secret Service implement a review process to ensure it accurately records cost data, and conduct an analysis of its domestic field office structure using cost and performance data. The Department of Homeland Security concurred.

Federal Protective Service: Enhancements to Performance Measures and Data Quality Processes Could Improve Human Capital Planning

Number: GAO-16-384
Date: 03/24/2016
Summary: The Federal Protective Service (FPS)—which protects about 9,500 federal facilities—developed a Strategic Human Capital Plan (Plan) and engaged in related efforts that generally align with most key principles GAO identified for strategic workforce planning. Specifically, FPS:

- solicited input from key stakeholders, such as its employees and the National Protection and Programs Directorate (NPPD)—FPS's parent organization responsible for managing and overseeing FPS's human capital efforts;
- determined critical skills and competencies;
- developed human capital strategies (i.e., programs, policies, and processes) tailored to address identified gaps and needs in its workforce; and
- identified actions that build the organizational capability to support the strategies.

However, FPS has not fully developed performance measures to evaluate progress toward goals, which is also a key principle for strategic workforce planning. For example, FPS has not identified performance measures for all of the Plan's strategies, has not included targets for the identified performance measures (e.g., a desired target for the "attrition rate" measure), and has not linked the

measures to FPS's human capital goals. GAO's work on measuring program performance has found that targets and linkages are among the attributes of successful performance measures. FPS and NPPD officials said they plan on developing measures with targets and linkages but have not yet established time frames for completing these tasks. Without performance measures that have targets and linkages, it will be difficult for NPPD and FPS to assess whether the Plan and related efforts are helping achieve FPS's human capital goals and its facility protection mission.

FPS designed its staffing model—which identifies the federal workforce the agency needs to meet its mission—consistent with most key practices GAO identified for the design of staffing models, and FPS uses the model to help make management decisions. Specifically, FPS's model includes:

- work activities and the time required to perform them;
- facility risk levels, which determine the frequency with which FPS must complete facility security assessments; and
- input from key stakeholders, including NPPD and some regional officials.

FPS officials said they took steps, such as reviewing work hour estimates, to ensure the quality of data used in the model—another key practice. FPS currently uses the model to help make human capital planning and other management decisions, but NPPD and FPS have not identified time frames for updating the model since its last update in August 2013. Furthermore, FPS cannot assure data quality in future updates to the model because it has no documented process for ensuring data quality. Without time frames for updating the model and guidance on ensuring data quality, NPPD and FPS may not have accurate estimates of staffing needs to make management decisions.

To improve FPS's human capital planning, GAO recommends that the Secretary of DHS direct NPPD and FPS to identify time frames for developing performance measures with targets that are explicitly aligned to FPS's goals, establish a plan and time frames for updating its staffing model, and develop and document guidance for ensuring the quality of staffing model data. DHS concurred with GAO's recommendations and outlined steps it plans to take to address them.

DHS OIG Reports

2014 White House Fence Jumping Incident (Redacted)

Number: OIG-16-64
Date: 04/12/2016
Summary: On September 19, 2014, an intruder jumped over the North Fence of the White House Complex and entered the White House before Secret Service personnel could apprehend him. A confluence of technical problems with radios, security equipment, and notification systems, as well as problems associated with the White House's infrastructure and surrounding physical environment, impeded the protective response.

Although they may have only indirectly contributed to the events of that night, underlying and continuing resource and management issues are negatively affecting the Uniformed Division and, potentially, its ability to protect the White House and its occupants. In particular, the Uniformed Division is severely understaffed, which has led to inadequate training, fatigue, low morale, and

attrition. In addition, there is a lack of full and open communication and information sharing between management and Uniformed Division Officers.

The Secret Service has attempted to resolve technical issues, as well as some problems with Uniformed Division staffing and training. In most cases, it is too early to tell whether these actions will lead to more effective protective operations and whether the Secret Service can continue to fund and sustain the corrections and improvements. Overcoming more deeply rooted challenges will require diligence and the full commitment of Secret Service leadership. The Secret Service concurred with our recommendations.

U.S. Secret Service Needs to Upgrade Its Radio Systems

Number: OIG-16-20 (Revised)
Date: 01/22/2016
Summary: Secret Service has a dual mission of protection and criminal investigations. To support its protective mission, officers carry radios, which are their first line of communication for events such as fence jumpers, suspicious packages, or protests. These radio systems are critical for day-to-day protective operations.

Secret Service needs to upgrade the radio systems used around the White House complex, the Vice President's Residence, and Foreign Diplomatic Embassies. Secret Service records show that, on average, the radios and associated infrastructure are between [redacted] years old and may not be working as effectively as needed. If Secret Service continues to use these outdated radio communications systems, it may negatively impact their protective operations.

Secret Service requested funding to upgrade these systems. By fiscal year 2019, Secret Service plans to invest about $54.2 million to upgrade its radio systems in the Washington, DC, area. This amount does not include what Secret Service will need to update its other radio systems. Secret Service acknowledged its need for updated radio equipment and concurred with our two recommendations in the report. At the request of Secret Service, here and throughout the report, we redacted sensitive information which may reveal vulnerabilities of its radio systems.

The Secret Service Did Not Identify Best Practices and Lessons Learned from the 2011 White House Shooting Incident

Number: OIG-16-16
Date: 12/17/2015
Summary: The Secret Service responded immediately to a November 2011 incident in which shots fired from an assault rifle hit the White House and participated in the ensuing investigation. However, the Secret Service did not conduct a formal after action review or a detailed analysis of its protective operations or investigative response, so it is not clear whether protective policies were followed.

After the incident, the Secret Service spent at least $17 million to improve infrastructure around the White House and increase patrols; however, without a formal after action review and detailed

analysis, the Secret Service cannot be certain these changes were necessary, would have minimized the potential threat, or improved the response to the incident.

Although the Secret Service has conducted after action reviews, defining what should be included in such reviews and completing a detailed analysis would help the Secret Service determine causes, necessary corrective actions, and future requirements. It would also help ensure informed decisions about necessary changes and effective use of budget and resources. Our review of this incident also identified concerns about potential vulnerabilities related to chain-of-command communication, training, and radios. We are continuing to review the other two incidents and the Secret Service's actions, so we make no recommendations in this report; we will include our recommendations in our final report. The Secret Service responded with general comments, which we included in an appendix to this report, as well as technical comments, which we incorporated as appropriate.

The FPS Vehicle Fleet Is Not Managed Effectively

Number: OIG-16-02
Date: 10/21/2015
Summary: FPS is not managing its fleet effectively. FPS did not properly justify that its current fleet is necessary to carry out its operational mission. Specifically, FPS did not justify the need for: more vehicles than officers; administrative vehicles; larger sport utility vehicles; home-to-work miles in one region; and discretionary equipment added to vehicles. Additionally, FPS overpaid for law enforcement equipment packages, did not have standard operating procedures for fleet management, a sound vehicle allocation methodology, or accurate fleet data to make effective management decisions. The Department of Homeland Security (DHS) and the National Protection and Programs Directorate (NPPD) fleet managers did not provide sufficient oversight to ensure FPS complied with all Federal and departmental guidance. As a result, FPS cannot ensure it is operating the most cost-efficient fleet and potentially missed opportunities to save more than $2.5 million in fiscal year 2014. The Department concurred with all five of our recommendations and implemented corrective action plans to address the findings. We consider all recommendations resolved and open.

Mission 2: Secure and Manage Our Borders

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

GAO Reports

U.S. Customs and Border Protection: Review of the Staffing Analysis Report under the Border Patrol Agent Pay Reform Act of 2014

Number: GAO-16-606R
Date: 05/26/2016
Summary: The Border Patrol Agent Pay Reform Act of 2014 (BPAPRA) established a new overtime compensation system for Border Patrol agents at U.S. Customs and Border Protection (CBP), within the Department of Homeland Security (DHS). Under BPAPRA, Border Patrol agents individually elect and are subsequently assigned by the agency to one of three rates of pay commensurate with the amount of scheduled overtime the agents elect or are assigned to work (0, 1, or 2 hours of overtime per day, with a corresponding overtime pay supplement of 0, 12.5, or 25 percent, respectively). To inform and guide how CBP will implement this overtime pay reform, BPAPRA required that CBP conduct a comprehensive staffing analysis and submit a report to the Comptroller General not later than 1 year after the date of BPAPRA's enactment (enacted December 18, 2014). GAO received the report from CBP on January 20, 2016.

GAO found that in developing its report, CBP relied on agent hours worked in prior years—and Border Patrol management's judgment on required staffing for certain duty locations—to establish staffing baseline levels for the purposes of its report. CBP's analysis was informed in part by the agency's separate Manpower Requirements Determination (MRD) process, a 3 to 5 year implementation effort begun in fiscal year 2014 in response to congressional direction, which is intended to determine specific staffing requirements for each Border Patrol duty location in fiscal year 2017 and thereafter. At the time of the report's issuance, Border Patrol had not yet identified such staffing requirements. As a result, it is too early for GAO to determine the extent to which the MRD process will result in identification of future staffing requirements for each Border Patrol duty location and position. Further, CBP has not to date performed sensitivity or data reliability analyses on the data inputs used to develop the report's cost assumptions and calculations. Therefore, the sensitivity and reliability of the analysis's data inputs and calculated outputs are unknown.

CBP's report concluded that allowing all Border Patrol agents to elect the BPAPRA Level 1 or 2 rate of pay (1 or 2 hours of overtime per day with a corresponding 12.5 or 25 percent overtime pay supplement, respectively) will achieve overall cost savings and greater operational flexibility by assigning fewer personnel to 10 hour days as compared to hiring additional staff to work 8 hour days with no regularly scheduled overtime. This conclusion is based, in part, on CBP's analysis of

agent hours worked in prior years and qualitative narratives in the report explaining that assigning agents at certain non-field locations to the Basic rate of pay (no regularly scheduled overtime or corresponding pay supplement) would have a negative impact on Border Patrol management's ability to attract and retain experienced and qualified field agents (earning Level 1 or 2 rate of pay) for assignments at these locations, thereby potentially decreasing the operational capability of the agency.

Given the caveats identified in the report—such as the report's reliance on agent hours worked in prior years rather than developing specific staffing requirements for each Border Patrol duty location--updating the report's data inputs based on future analyses, to include assessing data sensitivity and reliability, will be important for determining whether the conclusions reached in the report remain valid to support future determinations of BPAPRA rates of pay for agents across all duty locations. According to CBP officials, their analysis of agent hours worked in prior fiscal years will be updated in future years as part of the MRD process, specifically in relation to the MRD's identification of future staffing requirements.

GAO did not making any recommendations.

Border Security: DHS Surveillance Technology Unmanned Aerial Systems and Other Assets

Number: GAO-16-671T
Date: 05/24/2016
Summary: GAO reported in March 2014 and April 2015 that U.S. Customs and Border Protection (CBP), within the Department of Homeland Security (DHS), had made progress in deploying programs under the Arizona Border Surveillance Technology Plan (the Plan), but could take additional actions to strengthen its management of the Plan and its related programs. Specifically, in March 2014 GAO reported that CBP's schedules and life-cycle cost estimates for the Plan and its three highest-cost programs—which represented 97 percent of the Plan's total estimated cost—met some but not all best practices. GAO recommended that CBP ensure that its schedules and cost estimates more fully address best practices, such as validating cost estimates with independent estimates, and DHS concurred. As of May 2016, CBP has initiated or completed deployment of technology for each of the three highest-cost programs under the Plan, and reported updating some program schedules and cost estimates. For example, in May 2016, CBP provided GAO with complete schedules for two of the programs, and GAO will be reviewing them to determine the extent to which they address GAO's recommendation. GAO also reported in March 2014 that CBP had identified mission benefits of technologies under the Plan, such as improved situational awareness, but had not developed key attributes for performance metrics for all technologies, as GAO recommended in November 2011. As of May 2015, CBP had identified a set of potential key attributes for performance metrics for deployed technologies and expected to complete its development of baselines for measures by the end of 2015. In March 2016, GAO reported that CBP was adjusting the completion date to incorporate pending test and evaluation results for recently deployed technologies under the Plan.

GAO's ongoing work on CBP's use of unmanned aerial systems (UAS) for border security shows that CBP operates nine Predator B aircraft in U.S. airspace in accordance with Federal Aviation

Administration (FAA) requirements. Specifically, CBP's Air and Marine Operations operates the aircraft in accordance with FAA certificates of waiver or authorization for a variety of activities, such as training flights and patrol missions to support the U.S. Border Patrol's (Border Patrol) efforts to detect and apprehend individuals illegally crossing into the United States between ports of entry. Predator B aircraft are currently equipped with a combination of video and radar sensors that provide information on cross-border illegal activities to supported agencies. CBP data show that over 80 percent of Predator B flight hours were in airspace encompassing border and coastal areas from fiscal years 2011 through 2015. CBP officials stated that airspace access and hazardous weather can affect CBP's ability to utilize Predator B aircraft for border security activities. GAO's ongoing work shows that CBP has deployed six tactical aerostats—relocatable unmanned buoyant craft tethered to the ground and equipped with cameras for capturing full-motion video—along the U.S.-Mexico border in south Texas to support Border Patrol. CBP operates three types of tactical aerostats, which vary in size and altitude of operation. CBP officials reported that airspace access, hazardous weather, and real estate (e.g., access to private property) can affect CBP's ability to deploy and utilize tactical aerostats. Border Patrol has taken actions to track the contribution of tactical aerostats to its mission activities.

GAO has previously made recommendations to DHS to improve its management of plans and programs for surveillance technologies and DHS generally agreed.

Southwest Border Security: Additional Actions Needed to Assess Resource Deployment and Progress

Number: GAO-16-465T
Date: 03/01/2016
Summary: U.S. Customs and Border Protection (CBP), within the Department of Homeland Security (DHS), has taken action to deploy various resources—including agents and technology—along the southwest border and assess those resources' contributions to border security. For example, in December 2012, GAO reported that CBP's Border Patrol scheduled agents for deployment differently across southwest border locations, and although in most locations less than half of Border Patrol apprehensions were made within five miles of the border in fiscal year 2011, Border Patrol had moved overall enforcement efforts closer to the border since the prior fiscal year. GAO also reported in December 2012, that Border Patrol tracked changes in the effectiveness rate for response to illegal activity across border locations to determine if the appropriate mix and placement of personnel and assets were deployed and used effectively, and took steps to improve the data quality issues that had precluded comparing performance results across locations at the time of GAO's review. For example, Border Patrol issued guidance in September 2012 for collecting and reporting data with a more standardized and consistent approach. DHS has reported the effectiveness rate as a performance measure in its Fiscal Year 2015-2017 Annual Performance Report.

Further, in March 2014, GAO reported that CBP had made progress in deploying programs under the Arizona Border Surveillance Technology Plan, but that CBP could strengthen its management and assessment of the plan's programs. GAO reported that while CBP had identified mission benefits of technologies to be deployed under the plan, the agency had not developed key attributes for performance metrics to identify the technologies' individual and collective contribution, as GAO had recommended in 2011. GAO also reported in 2014 that CBP officials stated that baselines for

each performance measure would be developed and that by the end of fiscal year 2016, CBP would establish a tool to explain the impact of technology and infrastructure on situational awareness in the border environment. CBP should complete these actions in order to fully assess its progress in implementing the plan and determine when mission benefits have been fully realized.

In December 2012, GAO reported on Border Patrol's efforts to develop performance goals and measures for assessing the progress of efforts to secure the border between ports of entry and informing the identification and allocation of border security resources. GAO reported that DHS had transitioned from a goal and measure related to the capability to detect, respond to, and address cross-border illegal activity to an interim performance goal and measure of apprehensions between the land border ports of entry beginning fiscal year 2011. GAO reported that this interim goal and measure did not inform program results or resource identification and allocation decisions, limiting DHS and congressional oversight and accountability. DHS concurred with GAO's recommendation that CBP develop milestones and time frames for the development of border security goals and measures and Border Patrol works to define a new overarching performance goal for achieving a low-risk border and develop associated performance measures. CBP should complete these actions in order to fully assess its capabilities and progress to secure the border.

GAO previously made recommendations for DHS to, among other things, (1) strengthen its management of technology plans and programs and (2) establish milestones and time frames for the development of border security goals and measures. DHS generally agreed and has actions underway to address the recommendations.

Border Security: Actions Needed by DHS to Address Long-Standing Challenges in Planning for a Biometric Exit System

Number: GAO-16-358T
Date: 01/20/2016
Summary: The Department of Homeland Security (DHS) faces long-standing challenges in developing a biometric exit system and reporting reliable overstay data. In July 2013, GAO reported that DHS had not fulfilled statutory requirements to implement a biometric exit capability and report data on overstays. As of January 2016, DHS has planning efforts underway but has not yet met these statutory requirements. Specifically, in May 2012, DHS internally reported recommendations to support planning for a biometric exit capability at airports. However, as of January 2016, the department has not yet fully addressed those recommendations. For example, DHS has not completed an evaluation framework that, among other things, assesses the value of collecting biometric data in addition to biographic data, as it recommended in May 2012. In July 2013, GAO recommended that DHS establish time frames and milestones for a biometric air exit evaluation framework to help guide its assessment efforts. DHS concurred with the recommendation, and has actions planned or underway to address it. Specifically, in January 2016, U.S. Customs and Border Protection (CBP) officials stated that they were continuing to develop an evaluation framework by developing metrics for measuring the performance and effectiveness of biometric air exit technologies.

Moreover, in July 2013, GAO reported that, according to DHS officials, the department's goal was to develop information about options for biometric air exit and report to Congress in time for the

fiscal year 2016 budget cycle regarding the benefits and costs associated with a biometric air exit system. GAO found that, without robust planning that includes time frames and milestones to develop and implement an evaluation framework, DHS lacked reasonable assurance that it would be able to provide an assessment to Congress as planned. As of January 2016, DHS is working to develop this report for Congress, and CBP officials told GAO they were unable to estimate when it would be completed. Since GAO's 2013 report, DHS has also implemented several projects to test and evaluate biometric air exit technologies. For example, in July 2015, CBP began testing a handheld mobile device to collect biographic and biometric exit data from randomly-selected, foreign national travelers at 10 selected airports. Finalizing the evaluation framework consistent with GAO's recommendation would help guide DHS's efforts to assess the benefits and costs of various air exit options.

GAO also reported in July 2013 that challenges in developing a biometric exit system, as well as weaknesses in departure data, have affected the reliability of DHS's data on overstays. Because of concerns about the reliability of the department's overstay data, neither DHS nor its predecessor has regularly reported annual overstay data to Congress since 1994. In July 2013, GAO found that, although DHS had taken action to strengthen its overstay data, DHS had not validated or tested the reliability of those actions and challenges to reporting reliable overstay data remained. GAO recommended that DHS assess and document the reliability of its overstay data, and DHS concurred with the recommendation. However, as of January 2016, DHS has not yet reported overstay data or documented its reliability, and DHS officials could not provide a time frame for when they would address GAO's recommendation. GAO previously made recommendations to DHS to establish time frames and milestones for a biometric air exit evaluation framework and assess the reliability of its overstay data. DHS concurred with the recommendations, and has actions underway to address them.

Firearms Trafficking: U.S. Efforts to Combat Firearms Trafficking to Mexico Have Improved, but Some Collaboration Challenges Remain

Number: GAO-16-223
Date: 01/11/2016
Summary: According to data from the Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), 73,684 firearms (about 70 percent) seized in Mexico and traced from 2009 to 2014 originated in the United States. ATF data also show that these firearms were most often purchased in Southwest border states and that about half of them were long guns (rifles and shotguns). According to Mexican government officials, high caliber rifles are the preferred weapon used by drug trafficking organizations. According to ATF data, most were purchased legally in gun shops and at gun shows in the United States, and then trafficked illegally to Mexico. U.S. and Mexican law enforcement officials also noted a new complicating factor in efforts to fight firearms trafficking is that weapons parts are being transported to Mexico to be later assembled into finished firearms, an activity that is much harder to track.

In 2009, GAO reported duplicative initiatives, and jurisdictional conflicts between ATF and the Department of Homeland Security's Immigration and Customs Enforcement (ICE). That year, in response to GAO's recommendations on these problems, ATF and ICE updated an interagency memorandum of understanding (MOU) to improve collaboration. ATF and ICE have taken several steps since then to improve coordination on efforts to combat firearms trafficking, such as joint

training exercises and conferences to ensure that agents are aware of the MOU and its jurisdictional parameters and collaboration requirements. However, GAO found that ATF and ICE do not regularly monitor the implementation of the MOU. In the absence of a mechanism to monitor MOU implementation and ensure that appropriate coordination is taking place between the two agencies, GAO found that gaps in information sharing and misunderstandings related to their roles and responsibilities persist.

The indicator used to track U.S. agencies' efforts to stem firearms trafficking to Mexico in the Office of National Drug Control Policy's (ONDCP) National Southwest Border Counternarcotics Strategy, by itself, does not adequately measure progress. ONDCP tracks progress based on the number of arms seized in Mexico and traced to the United States; however, this number does not reflect the total volume of firearms trafficked from the United States, and it does not take into account other key supporting agency actions and activities as measures.

GAO recommends that the Secretary of Homeland Security and the Attorney General of the United States take steps to formally monitor implementation of the 2009 MOU between ATF and ICE. GAO also recommends that ONDCP establish comprehensive indicators that more accurately reflect progress made in efforts to stem arms trafficking to Mexico. The Departments of Homeland Security and Justice, and ONDCP agreed with GAO's recommendations.

Office of National Drug Control Policy: Lack of Progress on Achieving National Strategy Goals

Number: GAO-16-257T
Date: 12/02/2015
Summary: GAO reported in March 2013 that the Office of National Drug Control Policy (ONDCP) and other agencies had not made progress toward achieving most of the goals in the 2010 National Drug Control Strategy (the Strategy) and ONDCP had established a new mechanism to monitor and assess progress. In the Strategy, ONDCP established seven goals related to reducing illicit drug use and its consequences to be achieved by 2015. As of March 2013, GAO's analysis showed that of the five goals for which primary data on results were available, one showed progress and four showed no progress. GAO also reported that ONDCP established a new monitoring system intended to provide information on progress toward Strategy goals and help identify performance gaps and options for improvement. At that time, the system was still in its early stages, and GAO reported that it could help increase accountability for improving progress. In November 2015, ONDCP issued its annual Strategy and performance report, which assess progress toward all seven goals. The Strategy shows progress in achieving one goal, no progress on three goals, and mixed progress on the other three goals. Overall, none of the goals in the Strategy have been fully achieved.

ONDCP has assessed the extent of overlap and potential for duplication across federal drug abuse prevention and treatment programs and identified opportunities for increased coordination, as GAO recommended in March 2013. According to ONDCP's July 2014 assessment, these programs generally serve distinct beneficiaries in distinct settings, which helps prevent overlap and duplication. However, ONDCP found that programs that provide drug abuse prevention and

treatment services to address homelessness would benefit from greater coordination. ONDCP noted that it was taking steps to address this issue.

GAO reported in April 2013 that ONDCP-funded High Intensity Drug Trafficking Area (HIDTA) Investigative Support Centers and four other types of field-based information sharing entities had overlapping analytical and investigative support activities. However, ONDCP and the Departments of Homeland Security (DHS) and Justice (DOJ)—the federal agencies that oversee or provide support to the five types of field-based entities—were not holding entities accountable for coordination or assessing opportunities to implement practices that could enhance coordination, reduce unnecessary overlap, and leverage resources. ONDCP agreed with GAO's recommendations to work with DHS and DOJ to develop measures and assess opportunities to enhance coordination of field-based entities. Since July 2015, the agencies have worked through an interagency committee to make plans for collecting data on field-based collaboration, but have not yet fully addressed GAO's recommendations.

ONDCP has connected each of the systems that HIDTAs use to coordinate law enforcement activities, as GAO recommended in April 2013. Specifically, GAO reported in 2013 that HIDTAs and Regional Information Sharing System centers operated three systems that duplicate the same function—identifying when different law enforcement entities may be conducting a similar enforcement action, such as a raid at the same location—resulting in some inefficiencies. In May 2015, ONDCP completed connecting all three systems, which helps reduce risks to officer safety and potentially lessens the burden on law enforcement agencies that were using multiple systems.

GAO has made prior recommendations to ONDCP to assess overlap in drug prevention and treatment programs; develop measures and assess opportunities to enhance coordination of field-based entities; and connect existing coordination systems. ONDCP concurred and reported actions taken or underway to address them. GAO is not making new recommendations in this testimony.

Unaccompanied Alien Children: Improved Evaluation Efforts Could Enhance Agency Programs to Reduce Migration from Central America

Number: GAO-16-163T
Date: 10/21/2015
Summary: GAO reported in July 2015 that U.S. agencies had sought to address causes of unaccompanied alien child (UAC) migration through recent programs, such as information campaigns to deter migration, developed in response to the migration increase and other long-standing efforts. The increase in migration since 2012 was likely triggered, according to U.S. officials, by several factors such as the increased presence and sophistication of child smugglers (known as coyotes) and confusion over U.S. immigration policy. Officials also noted that certain persistent conditions such as violence and poverty have worsened in certain countries. In addition to long-standing efforts, such as U.S. Agency for International Development (USAID) antipoverty programs, agencies had taken new actions. For example, Department of Homeland Security-led investigative units had increasingly sought to disrupt human smuggling operations.

GAO found that U.S. agencies located programs based on various factors, including long-term priorities such as targeting high-poverty and -crime areas, but adjusted to locate more programs in

high-migration communities. For example, Department of State (State) officials in Guatemala said they moved programs enhancing police anticrime capabilities into such communities, and USAID officials in El Salvador said they expanded to UAC migration-affected locations.

GAO found that most agencies had developed processes to assess the effectiveness of programs seeking to address UAC migration, but weaknesses existed in these processes for some anti-smuggling programs. For example, DHS had established performance measures, such as arrests, for units combating UAC smuggling, but had not established numeric or other types of targets for these measures, which would enable DHS to measure the units' progress. In addition, DHS and State had not always evaluated information campaigns intended to combat coyote misinformation. DHS launched its 2013 campaign in April, but launched its 2014 campaign in late June after migration levels peaked. Neither agency evaluated its 2014 campaign. DHS has reported that it plans to evaluate its ongoing campaign before the end of this year.

GAO's July 2015 report included recommendations that DHS and State integrate evaluations into their information campaigns intended to deter migration, and that DHS establish performance targets for its investigative units. DHS concurred with both recommendations, and said that it plans to evaluate its most recent campaign. State also concurred with the recommendation directed to it.

DHS OIG Reports

CBP Needs to Better Plan Its Implementation of the DHS Prison Rape Elimination Act Regulations

Number: OIG-16-51
Date: 03/31/2016
Summary: The DHS PREA regulations set standards for CBP to prevent, detect, and respond to sexual abuse and assault. The regulations also require CBP to complete audits of holding facilities that "house detainees overnight" by July 2018. Since DHS issued its PREA regulations, CBP has taken measures, including issuing its zero-tolerance policy and designating a full-time Prevention of Sexual Assault Coordinator, to ensure its offices, stakeholders, and managers are aware of CBP's roles and responsibilities. However, CBP's implementation actions lack adequate planning, a budget, a component-wide policy to coordinate the efforts of all offices and personnel, and criteria to determine which facilities should be defined as overnight facilities and therefore subject to audits. Further, at the time of our review, CBP had not determined the feasibility of securing a joint PREA audit contract with U.S. Immigration and Customs Enforcement. These problems may hinder CBP's implementation of the DHS PREA regulations and ultimately, its ability to meet PREA's goal to prevent, detect, and respond to sexual abuse and assault. CBP concurred with four of our recommendations and is taking steps to address them. CBP did not concur with one of our recommendations. Based on CBP's response to our draft report, we closed one recommendation. We consider three resolved and open and the remaining recommendation unresolved.

Conditions at CBP's Forward Operating Bases along the Southwest Border

Number: OIG-16-37
Date: 02/08/2016
Summary: Of the seven Forward Operating Bases we inspected along the southwest border, six have adequate living conditions. One Forward Operating Base has security issues, safety and health concerns, and inadequate living conditions. At the other six Forward Operating Bases, we identified security issues, such as inoperable security cameras, as well as an ongoing challenge to provide safe drinking water. In addition, we determined that CBP is not performing all required Forward Operating Base inspections or adequately documenting maintenance and repairs. Without regular inspections and timely maintenance and repairs, CBP cannot ensure it will continue to provide adequate security, safety, and living conditions for its personnel working at these remote facilities. CBP concurred with our recommendations and is taking steps to address them. Based on CBP's response to our draft report, we closed one recommendation. We consider two recommendations unresolved and the remaining three recommendations resolved and open.

Response to Allegations that a U.S. Customs and Border Protection Contractor Transport Detainees in Non-Air-Conditioned Vehicles (Redacted)

Number: OIG-16-25
Date: 01/27/2016
Summary: In June 2015, we received a hotline complaint that "due to repair cost," CBP's contractor in the Border Patrol's Tucson sector was transporting some detainees in non-air-conditioned vehicles. The complainant also alleged the contractor did not maintain some vehicles adequately and would hide "defective" vehicles from inspection. In August 2015, we conducted unannounced spot inspections of CBP's contractor's vehicles in the Tucson sector. The contractor did not hide vehicles from inspection. Through our inspections, we determined the contractor's vehicles could reach reasonable temperatures or were operating at reasonable temperatures; we also determined that CBP and its contractor had addressed previously known problems with inadequate vehicle air conditioning. Finally, we reviewed the contractor's maintenance program and determined the contractor has adequate policies, procedures, and processes to maintain detainee transport vehicles, and the Border Patrol's Tucson sector has sufficient oversight of the contractor's program.

Goal 2.2: Safeguard and Expedite Lawful Trade and Travel

GAO Reports

Antidumping and Countervailing Duties: CBP Action Needed to Reduce Duty Processing Errors and Mitigate Nonpayment Risk

Number: GAO-16-542
Date: 07/14/2016
Summary: GAO estimates that about $2.3 billion in antidumping (AD) and countervailing (CV) duties owed to the U.S. government were uncollected as of mid-May 2015, based on its analysis of AD/CV duty bills for goods entering the United States in fiscal years 2001–2014. U.S. Customs and Border Protection (CBP) reported that it does not expect to collect most of that debt. GAO found that most AD/CV duty bills were paid and that unpaid bills were concentrated among a small number of importers, with 20 accounting for about 50 percent of the $2.3 billion uncollected. CBP data show that most of those importers stopped importing before receiving their first AD/CV duty bill. As GAO has previously reported, the U.S. AD/CV duty system involves the retrospective assessment of duties, such that the final amount of AD/CV duties an importer owes can significantly exceed the initial amount paid at the estimated duty rate when the goods entered the country.

CBP has undertaken efforts to improve its collection of AD/CV duties or to protect against the risk of unpaid final duty bills through bonding, but these efforts have yielded limited results. For example, CBP launched an initiative to reduce processing errors that result in CBP closing duty bills at the initial duty rate rather than the final duty rate, such that the initial duty paid may be significantly higher or lower than the final duty amount owed. Though the initiative has shown positive results, as of May 2016, its application had been limited. In addition, CBP had not collected and analyzed data systematically to help it monitor and minimize these duty processing errors. As a result, CBP does not know the extent of these errors and cannot take timely or effective action and avoid the potential revenue loss they may represent.

CBP's limited analysis of the risk to revenue from potentially uncollectible AD/CV duties (nonpayment risk) misses opportunities to identify and mitigate nonpayment risk. The standard definition of risk with regard to some negative event that could occur includes both the likelihood of the event and the significance of the consequences if the event occurs; however, CBP does not attempt to assess either of these risk components for any given entry of goods subject to AD/CV duties. GAO's analysis, applying standard statistical methods, demonstrates that a more comprehensive analysis of CBP data related to AD/CV duties is feasible and could help CBP better identify key factors associated with nonpayment risk and take steps to mitigate it.

GAO recommends that CBP (1) issue guidance to collect and analyze data on a regular basis to find and address the causes of AD/CV duty liquidation errors and track progress; (2) regularly conduct a comprehensive risk analysis that considers likelihood as well as significance of risk factors related

to duty nonpayment; and (3) take steps to use its data and risk assessment strategically to mitigate AD/CV duty nonpayment consistent with U.S. law and international trade obligations. CBP concurred with all three recommendations.

DHS OIG Reports

CBP Needs Better Data to Justify Its Criminal Investigator Staffing

Number: OIG-16-75
Date: 04/29/2016
Summary: In January 2015, CBP converted 183 of its 212 investigative program specialists to new criminal investigative positions without determining the appropriate number of investigators needed to effectively and efficiently accomplish its mission. CBP cannot ensure the criminal investigators are appropriately classified because it did not properly assess major duties its criminal investigators perform, did not conduct an adequate analysis of its staffing needs, and did not develop performance measures to assess the effectiveness of its investigative operations.

Without a comprehensive process and analysis to determine the appropriate number of criminal investigators, CBP may have improperly spent the approximately $3.1 million it paid for criminal investigators' premium pay in fiscal year 2015. Furthermore, if CBP does not make any changes to the number of criminal investigator positions, we estimate that it will cost as much as $22.6 million over 5 years for premium Law Enforcement Availability Pay. CBP concurred with all five recommendations but raised issues about the audit's timing, the financial impact of converting its investigative program specialists to criminal investigators, and the number of criminal investigators needed to accomplish its mission.

CBP's Special Operations Group Program Cost and Effectiveness are Unknown

Number: OIG-16-34
Date: 01/29/2016
Summary: We determined that CBP does not have formal performance measures for its SOG program and does not track SOG's total program cost.

Federal guidance requires agencies to develop goals and objectives that are outcome oriented and integrated with a strategic plan. Federal managers are also required to establish and maintain internal controls to achieve the objectives of effective and efficient operations.

The incomplete records of SOG and other components of CBP that support SOG limited the determination of the SOG program's total cost. SOG program efficiency and effectiveness cannot be accurately determined without total program costs or formal performance measures. As a result, CBP may be missing opportunities to improve effectiveness and identify potential cost savings in the SOG program.

We made no recommendation regarding the lack of formal performance measures in the SOG program because U.S. Border Patrol is in the process of developing and implementing performance measures. CBP concurred with our recommendation. The recommendation is resolved and open.

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

GAO Reports

No GAO reports were available that aligned to this goal.

DHS OIG Reports

ICE and USCIS Could Improve Data Quality and Exchange to Help Identify Potential Human Trafficking Cases

Number: OIG-16-17
Date: 01/04/2016
Summary: Our match of ICE and USCIS data from 2005 to 2014 indicated that work and fiancé visas were the primary means by which 17 of 32 known traffickers brought victims into the United States. In addition, we determined that 274 subjects of ICE human trafficking investigations successfully petitioned USCIS to bring 425 family members and fiancés into the United States.

Available data could not confirm whether or not these cases actually involved human trafficking. ICE and USCIS could improve data quality to facilitate the ability to identify instances of human trafficking. For example, ICE had to extensively manipulate its case management system to provide reasonably reliable data for matching purposes. USCIS did not always collect names and other identifiers of human traffickers that victims provided in their visa applications. Further, USCIS employees did not routinely share with ICE the data they collected on potential human traffickers. Without concerted DHS efforts to collect and share information, the risk exists that some human traffickers may remain unidentified and free to abuse other individuals. ICE and USCIS concurred with all three recommendations. We considered recommendations 1 and 2 open and resolved and recommendation 3 open and unresolved.

Mission 3: Enforce and Administer Our Immigration Laws

Goal 3.1: Strengthen and Effectively Administer the Immigration System

GAO Reports

Immigration Benefits System: U.S. Citizenship and Immigration Services Can Improve Program Management

Number: GAO-16-467
Date: 07/07/2016
Summary: U.S. Citizenship and Immigration Services (USCIS) created a reliable updated estimate to project the Transformation Program's cost, but has experienced program management challenges. In particular, the program's cost estimate was well-documented and substantially comprehensive, accurate, and credible. However, among other things, software development and systems integration and testing for USCIS's Electronic Immigration System (USCIS ELIS) have not consistently been managed in line with the program's policies and guidance or with leading practices.

Regarding software development, the Transformation Program has produced some software increments, but is not consistently following its own guidance and leading practices. The software development model (Agile) adopted by the USCIS Transformation Program in 2012 includes practices aimed at continuous, incremental release of segments of software. Important practices for Agile defined in program policies, guidance, and leading practices include ensuring that the software meets expectations prior to being deployed, teams adhere to development principles, and development outcomes are defined. For example, the program has committed to a specific framework for software development, referred to as Scrum, but has deviated from the underlying practices and principles of this framework.

The Transformation Program has established an environment that allows for effective systems integration and testing and has planned for and performed some system testing. However, the program needs to improve its approach to system testing to help ensure that USCIS ELIS meets its intended goals and is consistent with agency guidance and leading practices. Among other things, the program needs to improve testing of the software code that comprises USCIS ELIS and ensure its approaches to interoperability and end user testing, respectively, meet leading practices. Collectively, these limitations have contributed to issues with USCIS ELIS after new software is released into production.

GAO is making 12 recommendations to improve Transformation Program management, including ensuring alignment among policy, guidance, and leading practices in areas such as Agile software development and systems integration and testing. DHS concurred with the recommendations.

Visa Waiver Program: DHS Should Take Steps to Ensure Timeliness of Information Needed to Protect U.S. National Security

Number: GAO-16-498
Date: 05/05/2016
Summary: All 38 countries participating in the Visa Waiver Program (VWP) have entered into required agreements, or their equivalents, to (1) report lost and stolen passports, (2) share identity information about known or suspected terrorists, and (3) share criminal history information. However, not all countries have shared information through the agreements. The Department of Homeland Security (DHS) reported that all VWP countries have reported passport information through the first agreement, but more than a third of VWP countries are not sharing terrorist identity information through the second agreement and more than a third of the countries have not yet shared criminal history information through the third agreement. While VWP countries may share information through other means, U.S. agency officials told GAO that information sharing through the agreements is essential for national security. In August 2015, DHS decided to require VWP countries to implement agreements to share terrorist identity and criminal history information; previously, VWP countries were required to enter into, but not to implement, these agreements. However, contrary to standard program management practices, DHS did not establish time frames for instituting the amended requirements. In December 2015, Congress passed a law requiring that VWP countries fully implement information-sharing agreements in order to participate in the program. Time frames for working with VWP countries to implement their agreements could help DHS enforce U.S. legal requirements and could strengthen DHS's ability to protect the United States and its citizens.

GAO's analysis of a nongeneralizeable sample of 12 internal DHS reports, each evaluating one VWP country, found the reports assessed the effects of the countries' participation on U.S. law enforcement, security, and immigration enforcement interests, as required by U.S. law. Since 2011, when GAO last reviewed the VWP, DHS has improved its timeliness in reporting to Congress at least once every 2 years its determinations of whether countries should continue in the program. Nonetheless, as of October 31, 2015, GAO found that about a quarter of DHS's most recent VWP congressional reports were submitted, or remained outstanding, 5 or more months past the statutory deadlines. As a result, Congress may lack timely information needed to conduct oversight of the VWP and assess whether further modifications are necessary to prevent terrorists from exploiting the program.

DHS should (1) specify time frames for working with VWP countries on the requirement to implement information-sharing agreements and (2) take steps to improve its timeliness in reporting to Congress on whether VWP countries should continue in the program. DHS concurred with the recommendations.

Immigrant Investor Program: Additional Actions Needed to Better Assess Fraud Risks and Report Economic Benefits

Number: GAO-16-431T
Date: 02/11/2016
Summary: In August 2015, GAO reported that the Department of Homeland Security's (DHS) U.S. Citizenship and Immigration Services (USCIS), which administers the Employment-Based Fifth Preference Immigrant Investor Program (EB-5 Program), had collaborated with its interagency partners to assess fraud and national security risks in the program in fiscal years 2012 and 2015. These assessments were onetime efforts; however, USCIS officials noted that fraud risks in the EB-5 Program are constantly evolving, and they continually identify new fraud schemes. USCIS did not have documented plans to conduct regular future risk assessments which could help inform efforts to identify and address evolving program risks. GAO recommended that USCIS plan and conduct regular future fraud risks assessments. DHS agreed, and as of February 2016, USCIS officials stated that they planned to complete an additional risk assessment by September 2016 and a minimum of one annually thereafter. GAO also reported in August 2015 that USCIS had taken steps to address the fraud risks it identified by enhancing its fraud risk management efforts; however, USCIS's information systems and processes limited its ability to collect and use data on EB-5 Program participants to address fraud risks in the program. For example, USCIS did not consistently enter some information it collected on participants in its information systems, such as name and date of birth, and this presented barriers to conducting basic electronic searches that could be analyzed for potential fraud. USCIS planned to collect and maintain more complete data in its new information system; however, the information system improvements with the potential to expand USCIS's fraud mitigation efforts were not to take effect until 2017 at the earliest. Given this time frame and gaps in USCIS's other information collection efforts, GAO recommended that USCIS develop a strategy to expand information collection in order to better position the agency to identify and mitigate potential fraud. DHS concurred, and in February 2016 USCIS officials stated that USCIS plans to develop such a strategy by the end of fiscal year 2016.

In August 2015, GAO reported that USCIS had increased its capacity to verify job creation by increasing the size and expertise of its workforce, among other actions. However, USCIS's methodology for reporting program outcomes and overall economic benefits was not valid and reliable because it may understate or overstate program benefits in certain instances as it is based on the minimum program requirements of 10 jobs and a $500,000 investment per investor instead of the number of jobs and investment amounts collected by USCIS on individual EB-5 Program forms. For example, total investment amounts are not adjusted downward to account for investors who do not complete the program or upward for investments of $1 million instead of $500,000. USCIS officials said they are not statutorily required to develop a more comprehensive assessment. However, tracking and analyzing data on jobs and investments reported on program forms would better position USCIS to more reliably assess and report on the EB-5 Program economic benefits. Accordingly, GAO recommended that USCIS track and report data that investors report and the agency verifies on its program forms for total investments and jobs created through the EB-5 Program. DHS agreed and plans to implement this recommendation by the end of fiscal year 2017.

In its August 2015 report, GAO recommended that USCIS, among other things, conduct regular future risk assessments, develop a strategy to expand information collection, and analyze data

collected on program forms to reliably report on economic benefits. DHS concurred with the recommendations and reported actions underway to address them.

DHS OIG Reports

Potentially Ineligible Individuals Have Been Granted U.S. Citizenship Because of Incomplete Fingerprint Records

Number: OIG-16-130
Date: 09/08/2016
Summary: USCIS granted U.S. citizenship to at least 858 individuals ordered deported or removed under another identity when, during the naturalization process, their digital fingerprint records were not available. The digital records were not available because although USCIS procedures require checking applicants' fingerprints against both the Department of Homeland Security's and the Federal Bureau of Investigation's (FBI) digital fingerprint repositories, neither contains all old fingerprint records. Not all old records were included in the DHS repository when it was being developed. Further, U.S. Immigration and Customs Enforcement (ICE) has identified, about 148,000 older fingerprint records that have not been digitized of aliens with final deportation orders or who are criminals or fugitives. The FBI repository is also missing records because, in the past, not all records taken during immigration encounters were forwarded to the FBI. As long as the older fingerprint records have not been digitized and included in the repositories, USCIS risks making naturalization decisions without complete information and, as a result, naturalizing additional individuals who may be ineligible for citizenship or who may be trying to obtain U.S. citizenship fraudulently.

As naturalized citizens, these individuals retain many of the rights and privileges of U.S. citizenship, including serving in law enforcement, obtaining a security clearance, and sponsoring other aliens' entry into the United States. ICE has investigated few of these naturalized citizens to determine whether they should be denaturalized, but is now taking steps to increase the number of cases to be investigated, particularly those who hold positions of public trust and who have security clearances. DHS concurred with both recommendations and has begun implementing corrective actions.

Oversight Review of the United States Citizenship and Immigration Services, Investigations Division

Number: OIG-16-96-IQO
Date: 06/06/2016
Summary: We determined that investigations conducted by the Investigations Division were generally thorough and complete. We, however, found issues related to the Division's placement within the organization, discrepancies in policy, adherence to policy, and the application of rights advisements. Additionally, we found that the criminal investigators assigned to the Division did not maintain the mandatory minimum number of hours required to receive Law Enforcement Availability Pay (LEAP) and that managers and investigators did not comply with LEAP

certification requirements. We issued 25 recommendations, USCIS concurred with 24 of those recommendations.

USCIS Response: USCIS will conduct two comprehensive updates to their investigative policies and their business processes. The Office of Security and Integrity (OSI) will complete a comprehensive agency-wide investigations policy update, including review and development of relevant management directives, instructions and/or internal procedures. The update will also include policies covering evidence, sworn statements, recording interviews, and evaluating prosecutorial merit of allegations. OSI will also conduct a comprehensive business process analysis of its investigatory practices that will include validation of an appropriate and reasonable timeframe for conducting an investigation and producing corresponding reports.

USCIS Automation of Immigration Benefits Processing Remains Ineffective

Number: OIG-16-48
Date: 03/09/2016
Summary: Technology is crucial for the United States Citizenship and Immigration Services (USCIS) to accomplish its mission. Since 2005, USCIS has worked to transform its paper-based processes into an integrated and automated immigration benefits processing environment. As we previously reported, past automation attempts have been hampered by ineffective planning, multiple changes in direction, and inconsistent stakeholder involvement.

Current USCIS efforts to automate immigration benefits processing also could be improved. Although USCIS deployed the Electronic Immigration System (ELIS) in May 2012, to date only two of approximately 90 types of immigration benefits and services are available for online customer filing. The current ELIS approach also has not ensured stakeholder involvement, performance metrics, system testing, or user support needed for ELIS to be effective.

As it struggles to address these issues, USCIS now estimates that it will take three more years—over four years longer than estimated—and an additional $1 billion to automate all benefit types as expected. Until USCIS fully implements ELIS with all the needed improvements, the agency will remain unable to achieve its workload processing, customer service, and national security goals. USCIS concurred with two of the four recommendations.

Goal 3.2: Prevent Unlawful Immigration

GAO Reports

Immigration Detention: Additional Actions Needed to Strengthen DHS Management of Short-Term Holding Facilities

Number: GAO-16-514
Date: 05/26/2016
Summary: The Department of Homeland Security's (DHS) U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) have standards for short-term holding facilities—which are generally designed to keep individuals in custody for 24 hours or less—and some processes to monitor compliance with the standards. For example, each component has policies governing the operation of holding facilities, and CBP has an annual Self-Inspection Program, which is designed to assess internal controls in all CBP operations, including holding facilities. However, U.S. Border Patrol, within CBP, and ICE do not have a process to fully assess data on the amount of time individuals are held in custody. Such a process could help these agencies in better understanding issues that GAO identified, such as data quality, level of compliance with agency standards, and factors impacting time in custody. For example, GAO identified potential irregularities with Border Patrol's fiscal year 2014 to 2015 time in custody data, due to, among other things, delays in agents recording individuals' "book-out" from holding facilities. In addition, although Border Patrol officials from 10 holding facilities GAO visited stated that time in custody rarely exceeds 72 hours, GAO noted that approximately 16 percent of Border Patrol's cases with complete data in fiscal years 2014 to 2015 exceeded this threshold. Developing and implementing a process to assess time in custody data, consistent with internal control standards, would provide Border Patrol and ICE with more visibility into the quality of their data, facility compliance with time in custody guidelines, and the factors impacting time in custody.

DHS has various mechanisms to obtain and address complaints related to holding facilities. Specifically, individuals can submit complaints directly to holding facilities or to one of various DHS entities, including the DHS Office of Inspector General (OIG) and Joint Intake Center (JIC). However, DHS and its components have not consistently communicated information to individuals in CBP and ICE holding facilities on these mechanisms. For example, during site visits to DHS holding facilities, GAO observed that the posters used to communicate DHS complaint mechanisms varied in their coverage. Providing guidance to holding facilities on which of DHS's various complaint mechanisms they should communicate to individuals in custody, consistent with internal control standards, would help DHS have better assurance that individuals in custody within holding facilities have received information on how to submit a complaint. DHS complaint mechanisms maintain data in various systems; however, most of these systems do not have a classification code for holding facilities to would allow users to readily identify the universe of complaints involving holding facilities and conduct trend analysis. For example, the JIC's complaint tracking system does not include a facility, facility type, or issue code related to holding facilities. GAO found that information identifying whether a complaint involved a holding facility may be located within narrative fields. Creating a classification code and conducting trend analysis on holding facility

complaints, consistent with internal control standards, would provide DHS with useful information for management decisions, including targeting areas for compliance monitoring.

GAO recommends that DHS establish a process to assess time in custody data for all individuals in holding facilities; issue guidance on how and which complaint mechanisms should be communicated to individuals in short-term custody; include a classification code in all complaint tracking systems related to DHS holding facilities; and develop a process for analyzing trends related to holding facility complaints. DHS concurred with the recommendations and identified planned actions.

Immigration Detention: Additional Actions Needed to Strengthen Management and Oversight of Detainee Medical Care

Number: GAO-16-231
Date: 02/29/2016
Summary: The Department of Homeland Security's (DHS) U.S. Immigration and Customs Enforcement (ICE) oversees basic on-site medical care at all facilities, as required by ICE detention standards, but does not maintain complete information about medical care costs. The ICE Health Service Corps (IHSC) provided direct care to detainees at 19 over-72-hour facilities and oversaw care at the remaining 146 non-IHSC-staffed facilities in fiscal year 2015. At all facilities, IHSC uses an electronic system, the Medical Payment Authorization (MedPAR) system, to approve or deny off-site care requests for detainees; such requests could include dental visits or surgical needs. IHSC uses a system different from MedPAR to track costs or amounts paid for off-site care. The use of separate systems limits ICE's ability to link approvals and payments. For example, the number of claims paid for fiscal years 2012 through 2014 did not correspond to the number of IHSC MedPAR approvals for requested services for the same time period. While there are valid reasons for these differences, such as that approvals and claims could be made in different fiscal years, establishing a mechanism to more fully ensure that payments for off-site care are supported by the appropriate authorizations could help ICE monitor medical care costs and better validate payments.

ICE conducts medical care compliance inspections at individual facilities, but conducts limited analyses of inspection data across facilities and over time. ICE uses seven oversight mechanisms to monitor facilities' compliance with medical care detention standards, such as facility inspections and on-site detention monitors. The combined use of these oversight mechanisms resulted in more than 99 percent of ICE's average daily population (ADP) of approximately 28,000 detainees being covered by two or more mechanisms in fiscal year 2015. ICE's priority has been to focus on local, facility-specific issues rather than perform overarching analyses. For example, ICE does not utilize the data gathered through these mechanisms in a way that examines overall trends in medical care deficiencies. Conducting analysis of oversight data over time, by detention standards, and across facilities, consistent with internal control standards, could strengthen ICE's ability to manage and oversee the provision of medical care across facility types.

DHS has various processes to obtain and address the hundreds of medical care complaints it receives annually. Specifically, detainees can submit complaints regarding medical care directly to facilities or to one of various DHS entities, including the Office of Inspector General and Office for Civil Rights and Civil Liberties. These entities generally determine whether to take their own action on the complaints or forward them to ICE for resolution. These entities maintain complaint

data in various ways, and IHSC, which is ultimately responsible for addressing medical complaints received, is developing and piloting a new system for managing tasks, including addressing complaints. However, internal control standards call for evaluation of performance over time, and it is unclear whether IHSC's new system will capture all medical complaints received by DHS or facilitate analyses of complaints over time and across facilities. Ensuring that a new tasking system would capture all complaints and facilitate analysis could improve DHS's decision-making for detainee medical care.

GAO recommends that DHS, among other things, ensure payments for medical care are supported by authorizations, conduct trend analyses of oversight data, and track all medical complaints received by DHS entities. DHS concurred with the recommendations and identified planned actions to address the recommendations.

DHS OIG Reports

Release of Jean Jacques from ICE Custody

Number: No Number Provided
Date: 06/16/2016
Summary: In conducting this review, we found that:

- After his release from state custody, Jacques was held in ICE custody for about 205 days. During this period of custody, the ICE Enforcement and Removal Operations (ERO) Boston Field office conducted two Post-Order Custody Reviews and decided to continue to hold Jacques in custody.
- During Jacques' detention, ERO Boston and the Headquarters-based Travel Document Unit (TDU) made three attempts to remove Jacques to Haiti. The removal efforts included setting up an interview between Jacques and a Haitian consulate official as well as completing a sworn statement signed by Jacques identifying, among other things, his Haitian family members.
- Because Jacques did not possess a Haitian identification document, the Haitian government rejected all three repatriation requests. While there are standard practices and informal arrangements regarding repatriation, there are no written agreements between the two countries on this issue. ICE could not retrieve Jacques' birth certificate from Haiti, as they are not public documents.
- As Jacques' period of detention approached 180 days, the ERO Headquarters Post Order Custody Review Unit (POCR Unit) conducted a custody determination assessment. Consistent with ICE policy following the Supreme Court's ruling in Zadvydas v. Davis, and 8 C.F.R. §§ 214.13 & 214.14, ERO officials determined that it could not continue to detain Jacques because, in their judgment, there was no significant likelihood of removal in the reasonably foreseeable future.

While not explicitly required by existing ICE policy, ERO could have taken some additional steps to achieve Jacques' removal to Haiti while Jacques was still in ICE custody. However, we cannot conclude that those steps would have resulted in Jacques' removal from the United States.

The OIG also identified broader issues affecting removal efforts:

- Removal policies, procedures, and guidelines do not appear to be effectively disseminated to field staff. Most of the ERO officers OIG spoke to in the field, for example, were unaware of the existence of the Detention and Removal Operations Policy and Procedure Manual (DROPPM), which contains guidelines for removal.
- The OIG also identified a disconnect between how headquarters and field officers viewed removal efforts. While officers at headquarters acknowledged that Haiti was one of the more cooperative countries in assisting with removals, the view by many officers in the field was that removal to Haiti was exceedingly difficult, if not impossible.

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

Homeland Security: FPS and GSA Should Strengthen Collaboration to Enhance Facility Security

Number: GAO-16-135
Date: 05/17/2016
Summary: The Federal Protective Service (FPS), within the Department of Homeland Security (DHS), and the General Services Administration (GSA) have taken some steps to improve collaboration, such as drafting a joint strategy. While each agency has some individual policies for collaboration, the two agencies have made limited progress in agreeing on several key practices as described below. Reaching agreement on these practices will help to enhance the agencies' ability to protect federal facilities and to improve day-to-day operations at the regional level.

As a result of not having key practices in place, regional officials said they were not aware of agreed upon collaborative policies and procedures to conduct day-to-day operations. GAO found that this created inefficiencies and security risks. For example, FPS officials told GAO that GSA did not coordinate with them on new construction intended for law enforcement tenants, and as a result, it was not suitable for law enforcement use. GSA officials told GAO that they did not have sufficient information from FPS about security plans for upcoming events and, therefore, were not able to inform tenants of necessary security measures.

GAO recommends that FPS and GSA take actions to improve their collaboration in several areas, including defining common outcomes, agreeing on roles and responsibilities, and communicating compatible policies and procedures. DHS specifically concurred with GAO's recommendations, and GSA agreed to work with FPS to address the findings.

Critical Infrastructure Protection: Federal Efforts to Address Electromagnetic Risks

Number: GAO-16-641T
Date: 05/17/2016
Summary: Key federal agencies have taken various actions to address electromagnetic risks to the electric grid, and some actions align with the recommendations made in 2008 by the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (EMP Commission). Since 2008, the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC) have taken actions such as establishing industry standards and federal guidelines, and completing EMP-related research reports. GAO found that their actions aligned with some of the EMP Commission recommendations related to the electric grid. For example, DHS developed EMP protection guidelines to help federal agencies and industry identify options for safeguarding critical communication equipment and control systems from an EMP attack. Further, agency actions and EMP Commission recommendations generally align with DHS and DOE critical infrastructure responsibilities, such as assessing risks and identifying key assets.

Additional opportunities exist to enhance federal efforts to address electromagnetic risks to the electric grid. Specifically, DHS has not identified internal roles and responsibilities for addressing electromagnetic risks, which has led to limited awareness of related activities within the department and reduced opportunity for coordination with external partners. Doing so could provide additional awareness of related activities and help ensure more effective collaboration with other federal agencies and industry stakeholders. Moreover, although DHS components have independently conducted some efforts to assess electromagnetic risks, DHS has not fully leveraged opportunities to collect key risk inputs—namely threat, vulnerability, and consequence information—to inform comprehensive risk assessments of electromagnetic events. Within DHS, there is recognition that space weather and power grid failure are significant risk events, which DHS officials have determined pose great risk to the security of the nation. Better collection of risk inputs, including additional leveraging of information available from stakeholders, could help to further inform DHS assessment of these risks. DHS and DOE also did not report taking any actions to identify critical electrical infrastructure assets, as called for in the National Infrastructure Protection Plan. Although FERC conducted a related effort in 2013, DHS and DOE were not involved and have unique knowledge and expertise that could be utilized to better ensure that key assets are adequately identified and all applicable elements of criticality are considered. Finally, DHS and DOE, in conjunction with industry, have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks. Such activities include identifying and prioritizing key research and development efforts, and evaluating potential mitigation options, including the cost-effectiveness of specific protective equipment. Enhanced coordination to determine key research priorities could help address some identified research gaps and may help alleviate concerns voiced by industry regarding the costs and potential adverse consequences on grid reliability that may be caused by implementation of such equipment.

Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention

Number: GAO-16-174T
Date: 10/21/2015
Summary: GAO reported in 2011 that several entities—the North American Electric Reliability Corporation (NERC), the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE)—had taken steps to help secure the electric grid. These included developing cybersecurity standards and other guidance to reduce risks.

While these were important efforts, GAO at that time also identified a number of challenges to securing the electricity grid against cyber threats:

- Monitoring implementation of cybersecurity standards: GAO found that FERC had not developed an approach, coordinated with other regulatory entities, to monitor the extent to which the electricity industry was following voluntary smart grid standards, including cybersecurity standards.
- Clarifying regulatory responsibilities: The nature of smart grid technology can blur traditional lines between the portions of the grid that are subject to federal or state regulation. In addition, regulators may be challenged in responding quickly to evolving cybersecurity threats.
- Taking a comprehensive approach to cybersecurity: Entities in the electricity industry (e.g., utilities) often focused on complying with regulations rather than taking a holistic and effective approach to cybersecurity.
- Ensuring that smart grid systems have built-in security features: Smart grid devices (e.g., meters) did not always have key security features such as the ability to record activity on systems or networks, which is important for detecting and analyzing attacks.
- Effectively sharing cybersecurity information: The electricity industry did not have a forum for effectively sharing information on cybersecurity vulnerabilities, incidents, threats, and best practices.
- Establishing cybersecurity metrics: The electricity industry lacked sufficient metrics for determining the extent to which investments in cybersecurity improved the security of smart grid systems.

Since 2011, additional efforts have been taken to improve cybersecurity in the sector. For example, in 2013, NERC issued updated standards to address these and other cybersecurity challenges. NIST also updated its smart grid cybersecurity standards in 2014. It has also developed a cybersecurity framework for critical infrastructure, and DHS and DOE have efforts under way to promote its adoption. In addition, FERC assessed whether these and other challenges should be addressed in its ongoing cybersecurity efforts. However, FERC did not coordinate with other regulators to identify strategies for monitoring compliance with voluntary cybersecurity standards in the industry, as GAO had recommended. As a result, FERC does not know the extent to which such standards have been adopted or whether they are effective. Given the increasing use of information and communications technology in the electricity subsector and the evolving nature of cyber threats, continued attention can help mitigate the risk these threats pose to the electricity grid.

In its 2011 report, GAO recommended that (1) NIST improve its cybersecurity standards, (2) FERC assess whether challenges identified by GAO should be addressed in ongoing cybersecurity efforts, and (3) FERC coordinate with other regulators to identify strategies for monitoring compliance with voluntary standards. The agencies agreed with the recommendations, but FERC has not taken steps to monitor compliance with voluntary standards.

Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity

Number: GAO-16-116T
Date: 10/08/2015
Summary: Similar to other critical infrastructures, the nation's ports face an evolving array of cyber-based threats. These can come from insiders, criminals, terrorists, or other hostile sources and may employ a variety of techniques or exploits, such as denial-of-service attacks and malicious software. By exploiting vulnerabilities in information and communications technologies supporting port operations, cyber-attacks can potentially disrupt the flow of commerce, endanger public safety, and facilitate the theft of valuable cargo.

In its June 2014 report, GAO determined that the Department of Homeland Security (DHS) and other stakeholders had taken limited steps to address cybersecurity in the maritime environment. Specifically:

- DHS's Coast Guard had not included cyber-related risks in its biennial assessment of risks to the maritime environment, as called for by federal policy. Specifically, the inputs into the 2012 risk assessment did not include cyber-related threats and vulnerabilities. Officials stated that they planned to address this gap in the 2014 revision of the assessment. However, when GAO recently reviewed the updated risk assessment, it noted that the assessments did not identify vulnerabilities of cyber-related assets, although it identified some cyber threats and their potential impacts.
- The Coast Guard also did not address cyber-related risks in its guidance for developing port area and port facility security plans. As a result, port and facility security plans that GAO reviewed generally did not include cyber threats or vulnerabilities. While Coast Guard officials noted that they planned to update the security plan guidance to include cyber-related elements, without a comprehensive risk assessment for the maritime environment, the plans may not address all relevant cyber-threats and vulnerabilities.
- The Coast Guard had helped to establish information-sharing mechanisms called for by federal policy, including a sector coordinating council, made up of private-sector stakeholders, and a government coordinating council, with representation from relevant federal agencies. However, these bodies shared cybersecurity-related information to a limited extent, and the sector coordinating council was disbanded in 2011. Thus, maritime stakeholders lacked a national-level forum for information sharing and coordination.
- DHS's Federal Emergency Management Agency (FEMA) identified enhancing cybersecurity capabilities as a priority for its port security grant program, which is to defray the costs of implementing security measures. However, FEMA's grant review process was not informed by Coast Guard cybersecurity subject matter expertise or a comprehensive assessment of cyber-related risks for the port environment. Consequently, there was an

increased risk that grants were not allocated to projects that would most effectively enhance security at the nation's ports.

GAO concluded that until DHS and other stakeholders take additional steps to address cybersecurity in the maritime environment—particularly by conducting a comprehensive risk assessment that includes cyber threats, vulnerabilities, and potential impacts—their efforts to help secure the maritime environment may be hindered. This in turn could increase the risk of a cyber-based disruption with potentially serious consequences.

In its June 2014 report on port cybersecurity, GAO recommended that the Coast Guard include cyber-risks in its updated risk assessment for the maritime environment, address cyber-risks in its guidance for port security plans, and consider reestablishing the sector coordinating council. GAO also recommended that FEMA ensure funding decisions for its port security grant program are informed by subject matter expertise and a comprehensive risk assessment. DHS has partially addressed two of these recommendations since GAO's report was issued.

Critical Infrastructure Protection: Federal Agencies Have Taken Actions to Address Electromagnetic Risks, but Opportunities Exist to Further Assess Risks and Strengthen Collaboration

Number: GAO-16-243
Date: 03/24/2016
Summary: Key federal agencies have taken various actions to address electromagnetic risks to the electric grid, and some actions align with the recommendations made in 2008 by the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (EMP Commission). Since 2008, the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC) have taken actions such as establishing industry standards and federal guidelines, and completing EMP-related research reports. GAO found that their actions aligned with some of the EMP Commission recommendations related to the electric grid. For example, DHS developed EMP protection guidelines to help federal agencies and industry identify options for safeguarding critical communication equipment and control systems from an EMP attack. Further, agency actions and EMP Commission recommendations generally align with DHS and DOE critical infrastructure responsibilities, such as assessing risks and identifying key assets.

Additional opportunities exist to enhance federal efforts to address electromagnetic risks to the electric grid. Specifically, DHS has not identified internal roles and responsibilities for addressing electromagnetic risks, which has led to limited awareness of related activities within the department and reduced opportunity for coordination with external partners. Doing so could provide additional awareness of related activities and help ensure more effective collaboration with other federal agencies and industry stakeholders. Moreover, although DHS components have independently conducted some efforts to assess electromagnetic risks, DHS has not fully leveraged opportunities to collect key risk inputs—namely threat, vulnerability, and consequence information—to inform comprehensive risk assessments of electromagnetic events. Within DHS, there is recognition that space weather and power grid failure are significant risk events, which DHS officials have determined pose great risk to the security of the nation. Better collection of risk inputs, including

additional leveraging of information available from stakeholders, could help to further inform DHS assessment of these risks. DHS and DOE also did not report taking any actions to identify critical electrical infrastructure assets, as called for in the National Infrastructure Protection Plan. Although FERC conducted a related effort in 2013, DHS and DOE were not involved and have unique knowledge and expertise that could be utilized to better ensure that key assets are adequately identified and all applicable elements of criticality are considered. Finally, DHS and DOE, in conjunction with industry, have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks. Such activities include identifying and prioritizing key research and development efforts, and evaluating potential mitigation options, including the cost-effectiveness of specific protective equipment. Enhanced coordination to determine key research priorities could help address some identified research gaps and may help alleviate concerns voiced by industry regarding the costs and potential adverse consequences on grid reliability that may be caused by implementation of such equipment.

GAO recommends that DHS identify internal roles to address electromagnetic risks, and collect additional risk inputs to further inform assessment efforts; that DHS and DOE collaborate to ensure critical electrical infrastructure assets are identified; and engage with industry stakeholders to identify and prioritize risk-management activities, such as research and development efforts, to address EMP risks to the grid. DHS and DOE concurred with our recommendations and identified planned actions to address the recommendations.

DHS OIG Reports

No OIG reports were available that aligned to this goal.

Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise

GAO Reports

Federal Information Security: Actions Needed to Address Challenges

Number: GAO-16-885T
Date: 09/16/2016
Summary: Cyber incidents affecting federal agencies have continued to grow, increasing about 1,300 percent from fiscal year 2006 to fiscal year 2015. Several laws and policies establish a framework for the federal government's information security and assign implementation and oversight responsibilities to key federal entities, including the Office of Management and Budget, executive branch agencies, and the Department of Homeland Security (DHS).

However, implementation of this framework has been inconsistent, and additional actions are needed:

- Effectively implement risk-based information security programs. Agencies have been challenged to fully and effectively establish and implement information security programs. They need to enhance capabilities to identify cyber threats, implement sustainable processes for securely configuring their computer assets, patch vulnerable systems and replace unsupported software, ensure comprehensive testing and evaluation of their security on a regular basis, and strengthen oversight of IT contractors.
- Improve capabilities for detecting, responding to, and mitigating cyber incidents. Even with strong security, organizations can continue to be victimized by attacks exploiting previously unknown vulnerabilities. To address this, DHS needs to expand the capabilities and adoption of its intrusion detection and prevention system, and agencies need to improve their practices for responding to cyber incidents and data breaches.
- Expand cyber workforce and training efforts. Ensuring that the government has a sufficient cybersecurity workforce with the right skills and training remains an ongoing challenge. Government-wide efforts are needed to better recruit and retain a qualified cybersecurity workforce and to improve workforce planning activities at agencies.

Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System

Number: GAO-16-294
Date: 01/28/2106
Summary: The Department of Homeland Security's (DHS) National Cybersecurity Protection System (NCPS) is partially, but not fully, meeting its stated system objectives:

- Intrusion detection: NCPS provides DHS with a limited ability to detect potentially malicious activity entering and exiting computer networks at federal agencies. Specifically, NCPS compares network traffic to known patterns of malicious data, or "signatures," but does not detect deviations from predefined baselines of normal network behavior. In addition, NCPS does not monitor several types of network traffic and its "signatures" do not address threats that exploit many common security vulnerabilities and thus may be less effective.
- Intrusion prevention: The capability of NCPS to prevent intrusions (e.g., blocking an e-mail determined to be malicious) is limited to the types of network traffic that it monitors. For example, the intrusion prevention function monitors and blocks e-mail. However, it does not address malicious content within web traffic, although DHS plans to deliver this capability in 2016.
- Analytics: NCPS supports a variety of data analytical tools, including a centralized platform for aggregating data and a capability for analyzing the characteristics of malicious code. In addition, DHS has further enhancements to this capability planned through 2018.
- Information sharing: DHS has yet to develop most of the planned functionality for NCPS's information-sharing capability, and requirements were only recently approved. Moreover, agencies and DHS did not always agree about whether notifications of potentially malicious activity had been sent or received, and agencies had mixed views about the usefulness of these notifications. Further, DHS did not always solicit—and agencies did not always provide—feedback on them.

In addition, while DHS has developed metrics for measuring the performance of NCPS, they do not gauge the quality, accuracy, or effectiveness of the system's intrusion detection and prevention capabilities. As a result, DHS is unable to describe the value provided by NCPS.

Regarding future stages of the system, DHS has identified needs for selected capabilities. However, it had not defined requirements for two capabilities: to detect (1) malware on customer agency internal networks or (2) threats entering and exiting cloud service providers. DHS also has not considered specific vulnerability information for agency information systems in making risk-based decisions about future intrusion prevention capabilities.

Federal agencies have adopted NCPS to varying degrees. The 23 agencies required to implement the intrusion detection capabilities had routed some traffic to NCPS intrusion detection sensors. However, only 5 of the 23 agencies were receiving intrusion prevention services, but DHS was working to overcome policy and implementation challenges. Further, agencies have not taken all the technical steps needed to implement the system, such as ensuring that all network traffic is being routed through NCPS sensors. This occurred in part because DHS has not provided network routing guidance to agencies. As a result, DHS has limited assurance regarding the effectiveness of the system.

GAO recommends that DHS take nine actions to enhance NCPS's capabilities for meeting its objectives, better define requirements for future capabilities, and develop network routing guidance. DHS concurred with GAO's recommendations.

Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress

Number: GAO-16-79
Date: 07/12/2016
Summary: GAO's prior work has shown the Department of Homeland Security (DHS) has made progress in addressing barriers to conducting voluntary assessments but guidance is needed for DHS's critical infrastructure (CI) vulnerability assessments activities and to address potential duplication and gaps. For example:

Determining why some industry partners do not participate in voluntary assessments. In May 2012, GAO reported that various factors influence whether CI owners and operators participate in voluntary assessments that DHS uses to identify security gaps and potential vulnerabilities, but that DHS did not systematically collect data on reasons why some owners and operators of high-priority CI declined to participate. GAO concluded that collecting data on the reason for declinations could help DHS take steps to enhance the overall security and resilience of high-priority CI crucial to national security, public health and safety, and the economy, and made a recommendation to that effect. DHS concurred and has taken steps to address the recommendation, including developing a tracking system in October 2013 to capture declinations.

Establishing guidance for areas of vulnerability covered by assessments. In September 2014, GAO reported that the vulnerability assessment tools and methods DHS offices and components use vary with respect to the areas of vulnerability—such as perimeter security—assessed depending on

which DHS office or component conducts or requires the assessment. As a result it was not clear what areas DHS believes should be included in its assessments. GAO recommended that DHS review its vulnerability assessments to identify the most important areas of vulnerability to be assessed, and establish guidance, among other things. DHS agreed and established a working group in August 2015 to address this recommendation. As of March 2016 these efforts were ongoing with a status update expected in the summer of 2016.

Addressing the potential for duplication, overlap, or gaps between and among the various efforts. In September 2014, GAO found overlapping assessment activities and reported that DHS lacks a department-wide process to facilitate coordination among the various offices and components that conduct vulnerability assessments or require assessments on the part of owners and operators. This could hinder the ability to identify gaps or potential duplication in DHS assessments. GAO identified opportunities for DHS to coordinate with other federal partners to share information regarding assessments. In response to GAO recommendations, DHS began a process of identifying the appropriate level of guidance to eliminate gaps or duplication in methods and to coordinate vulnerability assessments throughout the department. GAO also recommended that DHS identify key CI security-related assessment tools and methods used or offered by other federal agencies, analyze them to determine the areas they capture, and develop and provide guidance for what areas should be included in vulnerability assessments of CI that can be used by DHS and other CI partners in an integrated and coordinated manner. DHS agreed, and as of March 2016, established a working group to address GAO recommendations.

Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments but Additional Improvements are Needed

Number: GAO-16-791T
Date: 07/12/2016
Summary: GAO's prior work has shown the Department of Homeland Security (DHS) has made progress in addressing barriers to conducting voluntary assessments but guidance is needed for DHS's critical infrastructure (CI) vulnerability assessments activities and to address potential duplication and gaps. For example:

Determining why some industry partners do not participate in voluntary assessments: In May 2012, GAO reported that various factors influence whether CI owners and operators participate in voluntary assessments that DHS uses to identify security gaps and potential vulnerabilities, but that DHS did not systematically collect data on reasons why some owners and operators of high-priority CI declined to participate. GAO concluded that collecting data on the reason for declinations could help DHS take steps to enhance the overall security and resilience of high-priority CI crucial to national security, public health and safety, and the economy, and made a recommendation to that effect. DHS concurred and has taken steps to address the recommendation, including developing a tracking system in October 2013 to capture declinations.

Establishing guidance for areas of vulnerability covered by assessments: In September 2014, GAO reported that the vulnerability assessment tools and methods DHS offices and components use vary with respect to the areas of vulnerability—such as perimeter security—assessed depending on

which DHS office or component conducts or requires the assessment. As a result it was not clear what areas DHS believes should be included in its assessments. GAO recommended that DHS review its vulnerability assessments to identify the most important areas of vulnerability to be assessed, and establish guidance, among other things. DHS agreed and established a working group in August 2015 to address this recommendation. As of March 2016 these efforts were ongoing with a status update expected in the summer of 2016.

Addressing the potential for duplication, overlap, or gaps between and among the various efforts: In September 2014, GAO found overlapping assessment activities and reported that DHS lacks a department-wide process to facilitate coordination among the various offices and components that conduct vulnerability assessments or require assessments on the part of owners and operators. This could hinder the ability to identify gaps or potential duplication in DHS assessments. GAO identified opportunities for DHS to coordinate with other federal partners to share information regarding assessments. In response to GAO recommendations, DHS began a process of identifying the appropriate level of guidance to eliminate gaps or duplication in methods and to coordinate vulnerability assessments throughout the department. GAO also recommended that DHS identify key CI security-related assessment tools and methods used or offered by other federal agencies, analyze them to determine the areas they capture, and develop and provide guidance for what areas should be included in vulnerability assessments of CI that can be used by DHS and other CI partners in an integrated and coordinated manner. DHS agreed, and as of March 2016, established a working group to address GAO recommendations.

GAO made recommendations to DHS in prior reports to strengthen its assessment efforts. DHS agreed with these recommendations and reported actions or plans to address them. GAO will continue to monitor DHS efforts to address these recommendations.

Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress

Number: GAO-16-79
Date: 11/19/2015
Summary: Sector-specific agencies (SSA) determined the significance of cyber risk to networks and industrial control systems for all 15 of the sectors in the scope of GAO's review. Specifically, they determined that cyber risk was significant for 11 of 15 sectors. Although the SSAs for the remaining four sectors had not determined cyber risks to be significant during their 2010 sector-specific planning process, they subsequently reconsidered the significance of cyber risks to the sector. For example, commercial facilities sector–specific agency officials stated that they recognized cyber risk as a high-priority concern for the sector as part of the updated sector planning process. SSAs and their sector partners are to include an overview of current and emerging cyber risks in their updated sector-specific plans for 2015.

SSAs generally took actions to mitigate cyber risks and vulnerabilities for their respective sectors. SSAs developed, implemented, or supported efforts to enhance cybersecurity and mitigate cyber risk with activities that aligned with a majority of actions called for by the National Infrastructure Protection Plan (NIPP). SSAs for 12 of the 15 sectors had not identified incentives to promote cybersecurity in their sectors as proposed in the NIPP; however, the SSAs are participating in a working group to identify appropriate incentives. In addition, SSAs for 3 of 15 sectors had not yet

made significant progress in advancing cyber-based research and development within their sectors because it had not been an area of focus for their sector. Department of Homeland Security guidance for updating the sector-specific plans directs the SSAs to incorporate the NIPP's actions to guide their cyber risk mitigation activities, including cybersecurity-related actions to identify incentives and promote research and development.

All SSAs that GAO reviewed used multiple public-private and cross-sector collaboration mechanisms to facilitate the sharing of cybersecurity-related information. For example, the SSAs used councils of federal and nonfederal stakeholders, including coordinating councils and cybersecurity and industrial control system working groups, to coordinate with each other. In addition, SSAs participated in the National Cybersecurity and Communications Integration Center, a national center at the Department of Homeland Security, to receive and disseminate cyber-related information for public and private sector partners.

The Departments of Defense, Energy, and Health and Human Services established performance metrics for their three sectors. However, the SSAs for the other 12 sectors had not developed metrics to measure and report on the effectiveness of all of their cyber risk mitigation activities or their sectors' cybersecurity posture. This was because, among other reasons, the SSAs rely on their private sector partners to voluntarily share information needed to measure efforts. The NIPP directs SSAs and their sector partners to identify high-level outcomes to facilitate progress towards national goals and priorities. Until SSAs develop performance metrics and collect data to report on the progress of their efforts to enhance the sectors' cybersecurity posture, they may be unable to adequately monitor the effectiveness of their cyber risk mitigation activities and document the resulting sector-wide cybersecurity progress.

GAO recommends that certain SSAs collaborate with sector partners to develop performance metrics and determine how to overcome challenges to reporting the results of their cyber risk mitigation activities. Four of these agencies concurred with GAO's recommendation, while two agencies did not comment on the recommendations.

Information Security: Federal Agencies Need to Better Protect Sensitive Data

Number: GAO-16-194T
Date: 11/17/15
Summary: Federal systems face an evolving array of cyber-based threats. These threats can be unintentional—for example, from software coding errors or the actions of careless or poorly trained employees; or intentional—targeted or untargeted attacks from criminals, hackers, adversarial nations, terrorists, disgruntled employees or other organizational insiders, among others. These concerns are further highlighted by recent incidents involving breaches of sensitive data and the sharp increase in information security incidents reported by federal agencies over the last several years, which have risen from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014.

Security control weaknesses place sensitive data at risk. GAO has identified a number of deficiencies at federal agencies that pose threats to their information and systems. For example, agencies, including the Department of Homeland Security, have weaknesses with the design and

implementation of information security controls, as illustrated by 19 of 24 agencies covered by the Chief Financial Officers Act declaring cybersecurity as a significant deficiency or material weakness for fiscal year 2014. In addition, most of the 24 agencies continue to have weaknesses in key controls such as those for limiting, preventing, and detecting inappropriate access to computer resources and managing the configurations of software and hardware.

Until federal agencies take actions to address these weaknesses—including implementing the thousands of recommendations GAO and agency inspectors general have made—federal systems and information will be at an increased risk of compromise from cyber-based attacks and other threats.

DHS OIG Reports

Review of the Department of Homeland Security's Implementation of the Cybersecurity Act of 2015

Number: OIG-16-142
Date: 09/26/2016
Summary: The Department has taken a number of steps to implement provisions in Title IV, Section 406 of the Cybersecurity Act. As required by the Act, we examined DHS activities in four key cybersecurity areas. We determined the Department has—

- developed enterprise-wide logical access policies and procedures for its NSS and other systems that provide access to PII, in accordance with appropriate Federal standards;
- applied its process for authorizing systems to operate to ensure logical access controls are implemented and assessed, and ensured multi-factor authentication for privileged users of unclassified systems, and some NSS;
- established software inventory policies, although not all DHS components used data exfiltration protection capabilities to support data loss prevention, forensics and visibility, and digital rights management; and
- not developed policies and procedures to ensure that contractors implement data protection solutions.

DHS and its Components can benefit from additional data protection capabilities and policy to help ensure sensitive PII and classified information are secure from unauthorized access, use, and disclosure. We are submitting this report for informational purposes to the appropriate Congressional oversight committees, as required by the Act. Due to a lack of specific criteria, this report contains no recommendations.

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

GAO Reports

No GAO reports were available that aligned to this goal.

DHS OIG Reports

No OIG reports were available that aligned to this goal.

Goal 4.4: Strengthen the Cyber Ecosystem

GAO Reports

No GAO reports were available that aligned to this goal.

DHS OIG Reports

No OIG reports were available that aligned to this goal.

Mission 5: Strengthen National Preparedness and Resilience

Goal 5.1: Enhance National Preparedness

GAO Reports

Emergency Management: Improved Federal Coordination Could Better Assist K-12 Schools Prepare for Emergencies

Number: GAO-16-144
Date: 03/10/2016
Summary: The Departments of Education (Education), Health and Human Services (HHS), Homeland Security (DHS), and Justice (Justice) support K-12 schools in preparing for emergencies with various resources, including training, technical assistance, and funding, but their efforts are not strategically coordinated. Since jointly issuing a Guide for Developing High-Quality School Emergency Operations Plans in 2013 in response to a presidential plan, individual agencies have continued to work on a range of emergency preparedness initiatives, sometimes collaboratively; however, with the guide completed and no strategic coordination of agency efforts particular to schools, federal agencies have taken a piecemeal approach to their efforts. GAO found gaps in coordination that suggest recent efforts are insufficient: not all relevant agencies and officials are included in collaborative efforts or are aware of related efforts and resources, and agencies are offering different interpretations of the same federal guidance—all of which risks wasting limited federal resources on duplicative, overlapping, or fragmented efforts. Education officials said that although agencies discussed the need to continue coordinating following the guide, the presidential plan did not designate a lead agency going forward, nor give any agency direct authority or responsibility over an interagency effort, or require agency participation. However, these officials said Education has general authority to collaborate with other federal agencies to maximize the efficiency and effectiveness of its programs and to serve as the lead agency, where warranted and agreed upon. Leading practices on federal interagency collaboration include identifying leadership, relevant participants, and resources, and agreeing on outcomes. Absent a well-coordinated effort, agencies will continue to determine their priorities individually, which may hinder assistance to schools.

In GAO's survey of 51 state educational agencies, 32 states reported that they require districts to have emergency operations plans, 34 reported they require schools to have plans, and almost all states reported providing training, technical assistance, or guidance to support districts in developing or implementing plans. GAO's survey also found that 32 states reported requiring districts to conduct emergency exercises, such as drills, and 40 states reported requiring individual schools to do so. In addition, many states reported allowing districts and schools to determine specific plan content, with fewer than half reporting that they required districts or states to review district or school plans.

GAO's generalizable survey of school districts estimates that most districts updated and practiced their emergency operations plans with first responders, but struggled to balance emergency planning with other priorities. GAO's survey results also found that most districts had plans addressing multiple hazards and emergency procedures, such as evacuation. However, GAO estimates about half of districts included procedures on continuing operations or recovering after an incident. GAO also found most districts conducted emergency exercises, such as fire drills, and about half did so annually with police and fire department officials. However, an estimated 59 percent of districts had difficulty balancing emergency planning with higher priorities, such as classroom instruction time.

GAO recommends that Education convene its federal interagency partners to develop a strategic approach to interagency collaboration on school emergency preparedness, consistent with leading practices. Education agreed that such improved federal coordination will better assist schools in preparing for emergencies.

Emergency Communications: Actions Needed to Better Coordinate Federal Efforts in the National Capital Region

Number: GAO-16-249
Date: 03/10/2016
Summary: The Office of National Capital Region Coordination (ONCRC), within the Department of Homeland Security (DHS), has taken various actions, mainly through coordination with state and local agencies, to help improve emergency communications interoperability in the National Capital Region (NCR), a legally-designated area including Washington, D.C. and nearby parts of Virginia and Maryland. For example:

- The ONCRC participates in several committees that are involved in planning and carrying out efforts to build preparedness and response capabilities of the region. In particular, the Director of the ONCRC is a member of the NCR's Senior Policy Group, which coordinates these efforts. The ONCRC staff helped develop the NCR's 2013 Homeland Security Strategic Plan. One of the goals of the plan is to ensure interoperable communications capabilities. The Strategic Plan identified a number of NCR initiatives to achieve this goal, including supporting the establishment and maintenance of radio interoperability and managing and coordinating radio upgrades across jurisdictions.
- As part of the responsibility to serve as a liaison with entities in the NCR, the ONCRC has collaborated with the NCR's Emergency Preparedness Council (an NCR advisory body) to facilitate state and local agencies access to the DHS's Urban Area Security Initiative grant program—the primary source of federal homeland security funding for the NCR. In fiscal year 2014, DHS allocated $53 million in grant funding to the NCR to enhance the region's homeland security and preparedness capabilities. Almost $7 million of this amount was to fund activities, such as purchasing radios and other equipment, aimed at achieving the NCR Strategic Plan's goal to ensure interoperable communications capabilities.

A key role of the ONCRC is to coordinate with federal, state, and local NCR entities on emergency preparedness and homeland security activities. However, the ONCRC currently does not have a formal mechanism in place to coordinate with federal agencies. From 2002 through 2014, the Joint

Federal Committee (JFC) was the ONCRC's primary means of coordinating with federal agencies in the NCR. The ONCRC has not convened the JFC since 2014 and plans to restructure it. Officials explained that the JFC was not efficient and effective as a coordinating body and that they plan to strengthen its coordination capabilities. However, written plans were not available. When the JFC existed, its operation was not fully aligned with interagency collaboration mechanisms that GAO has identified. In particular, the JFC's charter did not specify the roles and responsibilities of participating agencies or how they were to work together across agency boundaries. Addressing these interagency collaborative mechanisms in the planned restructuring of the JFC could provide greater clarity on roles and responsibilities and enhance its ability to coordinate federal efforts in the region.

GAO recommends that ONCRC, as part of its efforts to restructure the JFC, clearly articulate in a written agreement the roles and responsibilities of participating agencies and specify how they are to work together across agency boundaries. ONCRC concurred with this recommendation.

DHS OIG Reports

FEMA Should Implement Consistent Joint Field Office Guidance

Number: OIG-16-139-D
Date: 09/27/2016
Summary: Since 2012, we have observed and reported on systemic challenges in FEMA's JFO selection process. These challenges occurred, in part, because FEMA has not sufficiently implemented our prior audit recommendation to collaborate with the General Services Administration in selecting potential JFO sites prior to a forecasted disaster.

In 2015, we identified regional implementation differences in the JFO selection process. During our 2015 Texas flood disaster Emergency Management Oversight Team (EMOT) deployment, we determined that FEMA Region VI did not implement a disaster pre-planning protocol that resulted in a more than $380,000 increase in JFO administrative costs and delayed the JFO opening by 17 days. The delayed JFO opening negatively impacted FEMA's ability to rapidly equip and deploy disaster response personnel. In contrast, during our 2015 South Carolina EMOT deployment, we determined that FEMA Region IV JFO selection was efficient and effective. FEMA concurred with our recommendations.

FEMA Can Enhance Readiness with Management of Its Disaster Incident Workforce

Number: OIG-16-127-D
Date: 09/02/2016
Summary: Despite recent hiring initiatives, FEMA's disaster incident workforce remains significantly understaffed, and some Reservists continue to deploy to disasters without the knowledge, skills, and training they need to assist survivors effectively. Maintaining the skills of an intermittent on-call workforce will always be challenging; however, FEMA can take steps to improve the skills, knowledge, and morale of its Reservist workforce. These steps should include developing a more rigorous FEMA Qualification System-based performance evaluation system;

increasing training opportunities for Reservists when not deployed; improving communication between Reservists and their managers; taking a greater role in assessing Reservists' performance; promoting their professional development; and engaging all FEMA components, including the FEMA Regions, to strengthen the Reservist workforce.

Reservists comprise the largest part of FEMA's disaster incident workforce, yet FEMA has hired less than half the Reservists it needs based on its target staffing goals. FEMA's success in responding to the next catastrophic disaster or to simultaneous, large disasters will depend in part on the performance of its Reservists. However improved, Reservist performance and morale will be of little consequence if FEMA does not have enough trained and experienced Reservists ready to respond to the next catastrophic disaster. FEMA concurred with all four recommendations and is committed to building and maintaining a well-trained, adequately staffed workforce.

Audit Tips For Managing Disaster-Related Project Costs

Number: OIG-16-109-D
Date: 07/01/2016
Summary: More than 148,000 recipients and sub-recipients of FEMA disaster assistance grants are currently working on about 670,000 open projects worth over $66 billion. Under the Public Assistance Program, FEMA provides grants to state, tribal, and local governments and private nonprofit organizations so that communities can quickly respond to and recover from major disasters. FEMA's Hazard Mitigation Grant Program provides funding to the same entities to implement long-term measures to prevent damages from future disasters. Using this report will assist Disaster Assistance applicants:

- document and account for disaster-related costs;
- minimize the loss of FEMA disaster assistance funds;
- maximize financial recovery; and
- prevent fraud, waste, and abuse of disaster funds.

Response to Allegations of Mismanagement in FEMA's Office of the Chief Security Office

Number: OIG-16-41
Date: 02/19/2016
Summary: In 2011, the former FEMA Chief Security Officer hired two employees with criminal convictions in their backgrounds. Our analysis of employee records from 2011 to 2014 in the Office of the Chief Security Officer's Fraud and Internal Investigations Division disclosed two more employees with criminal conduct in their backgrounds. FEMA's Office of the Chief Security Officer no longer employs these four individuals. FEMA premium pay records from 2011 to 2014 for employees in the Fraud and Internal Investigations Division showed that division management allowed employees to violate FEMA's premium pay policy for compensatory time in 2014; premium pay requests from the same period did not reveal any overtime violations. As a result of hiring employees with criminal backgrounds or conduct, the Office of the Chief Security Officer spent $349,944 unnecessarily. Finally, from 2013 to 2014, the Office of the Chief Security Officer misused the Disaster Relief Fund by allowing employees to perform non-disaster related activities, which violates the Stafford Act and may also be a potential Antideficiency Act violation. FEMA

officials concurred with both recommendations, and FEMA has taken steps to improve the functioning of its Office of the Chief Security Officer. Also, DHS' Chief Financial Officer will lead an investigation to determine whether an Antideficiency Act violation occurred. We consider recommendation 1 resolved and closed and recommendation 2 resolved and open.

Clearer Guidance Would Improve FEMA's Oversight of the Public Assistance Alternative Procedures Pilot Program

Number: OIG-16-03-D
Date: 10/27/12015
Summary: The Federal Emergency Management Agency's (FEMA) Program Guide for the Alternative Procedures pilot program and letters of undertaking provide acceptable guidance in most areas to ensure compliance with Federal rules and regulations. However, our review of seven large dollar value projects valued at $3.9 billion identified weaknesses in five areas of guidance:

1. estimating project costs;
2. responding to Office of Inspector General (OIG) audits;
3. managing cash responsibly;
4. applying insurance proceeds; and
5. obtaining insurance for future losses.

These weaknesses put Federal funds at greater risk of fraud, waste, and abuse. Correcting these weaknesses will better ensure that participants in the pilot program will follow Federal requirements when spending Federal funds. Further, to protect the Federal taxpayer from inflated estimates, FEMA's oversight should include additional steps to assess the accuracy of subgrantee fixed-cost estimates that exceed certain thresholds. In addition, FEMA needs to make other changes to comply with the Stafford Act and protect the integrity of the program. FEMA Response
FEMA concurred with the three recommendations in the report and acted promptly to address a number of issues identified in the report. FEMA intends to address other findings with updates to its guidance and applicant letters.

Goal 5.2: Mitigate Hazards and Vulnerabilities

GAO Reports

No GAO reports were available that aligned to this goal.

DHS OIG Reports

FEMA's Grant Programs Directorate Did Not Effectively Manage Assistance to Firefighters Grant Program - AFG Grants

Number: OIG-16-100
Date: 06/09/2016
Summary: Sixty-four percent (243 of 379) of AFG grant recipients (grantees) we reviewed did not comply with grant guidance and requirements to prevent waste, fraud, and abuse of grant funds. AFG grant appropriations for fiscal years 2010 through 2012 totaled approximately $1.13 billion. We examined about $50 million in grant funds spent and are questioning $7.1 million.

FEMA's GPD did not sufficiently manage or oversee the Program's administration of AFG grants and did not effectively control the risk of fraud, waste, abuse, and grant mismanagement. FEMA cannot assure grant funds were used to help local fire departments and other first responder organizations obtain equipment, protective gear, emergency vehicles, training, and other resources. FEMA concurred with and has taken corrective actions to resolve both recommendations.

FEMA's Grant Programs Directorate Did Not Effectively Manage Assistance to Firefighters Grant Program - SAFER Grants

Number: OIG-16-98
Date: 06/08/2016
Summary: Sixty-three percent (88 of 139) of SAFER grant recipients (grantees) we reviewed did not comply with grant guidance and requirements to prevent waste, fraud, and abuse of grant funds. SAFER grant appropriations for fiscal years 2010 through 2012 totaled approximately $1.16 billion. We examined about $72 million in grant funds spent and are questioning $18.4 million.

FEMA's GPD did not sufficiently manage or oversee the Program's administration of SAFER grants and did not effectively control the risk of fraud, waste, abuse, and grant mismanagement. FEMA cannot assure grant funds were used to help local fire departments and other first responder organizations hire and retain firefighters, obtain equipment, and provide training. FEMA concurred with and has taken corrective actions to resolve both recommendations.

Analysis of Recurring Audit Recommendations Could Improve FEMA's Oversight of HSGP

Number: OIG-16-49
Date: 03/15/2016
Summary: FEMA has not adequately analyzed recurring Office of Inspector General recommendations to implement permanent changes to improve its oversight of HSGP. This occurred because FEMA has not clearly communicated internal roles and responsibilities, and does not have policies and procedures for conducting substantive trend analysis of audit recommendations. Office of Management and Budget (OMB) Circular A50 (revised) directs

executive agencies to "provide for periodic analysis of audit recommendations, resolution, and corrective action, to determine trends and system-wide problems, and to recommend solutions." Without sufficiently analyzing audit findings and recommendations, FEMA may not be able to develop proactive solutions to recurring and systemic problems, resulting in missed opportunities to improve the management and oversight of its HSGP. FEMA concurred with our report recommendation and provided a corrective action plan to address it.

FEMA Does Not Provide Adequate Oversight of Its National Flood Insurance Write Your Own Program

Number: OIG-16-47
Date: 03/08/2016
Summary: FEMA does not provide adequate oversight of the WYO program under the National Flood Insurance Program (NFIP). Specifically, FEMA is not using the results from its Financial Control Plan reviews to make program improvements; is not performing adequate oversight of the Special Allocated Loss Adjustment Expense reimbursement process; and does not have adequate internal controls to provide proper oversight of the appeals process. These conditions exist because FEMA does not have adequate guidance, resources, or internal controls. As a result of this inadequate oversight, FEMA is unable to ensure that WYO companies are properly implementing the NFIP and is unable to identify systemic problems in the program. Furthermore, without adequate internal controls in place, FEMA's NFIP funds may be at risk for fraud, waste, abuse, or mismanagement. FEMA concurred with all seven of our recommendations and has already begun implementing corrective actions.

Goal 5.3: Ensure Effective Emergency Response

GAO Reports

Emergency Communications: Effectiveness of the Post-Katrina Interagency Coordination Group Could Be Enhanced

Number: GAO-16-681
Date: 07/14/2016
Summary: Implementation of the Post-Katrina Emergency Management Reform Act of 2006 (PKEMRA) provisions related to emergency communications planning and federal coordination has enhanced federal support for state and local efforts; however, federal coordination could be improved. PKEMRA created within the Department of Homeland Security (DHS) the Office of Emergency Communications, which has taken a number of steps aimed at ensuring that state and local agencies have the plans, resources, and training they need to support reliable emergency communications. PKEMRA also directed DHS to develop the National Emergency Communications Plan (NECP). The NECP includes goals for improving emergency communications and encourages states to align their plans with these emergency communications goals. PKEMRA further established the Emergency Communications Preparedness Center (ECPC),

comprising 14 member agencies, to improve coordination and information sharing among federal emergency communications programs. GAO previously identified key features and issues to consider when implementing collaborative mechanisms, including interagency groups like the ECPC. GAO found that the ECPC's collaborative efforts were consistent with most of these features, such as those related to leadership and resources, but were not fully consistent with others. For example, one of the key features calls for interagency groups to clearly define goals and track progress, yet the ECPC has not done so. As a result, the ECPC's member agencies might not understand the ECPC's goals or have a chance to ensure that the goals align with their own agencies' purposes and goals. Furthermore, the ECPC puts forth recommendations that could improve emergency communications. But the recommendations are implemented at the discretion of the ECPC's member agencies and are not tracked. Without a mechanism to track the ECPC's recommendations, it is unclear the extent to which the recommendations are being implemented and the ECPC is missing an opportunity to monitor its progress.

Almost all of the Statewide Interoperability Coordinators (SWIC) responding to GAO's survey reported that to better plan for emergency communications during disasters, their states have taken the following steps since PKEMRA: (1) developed comprehensive strategic plans for emergency communications that align with the NECP; (2) established SWIC positions to support state emergency communications initiatives, such as developing high-level policy and coordinating training and exercises; and (3) implemented governance structures to manage the systems of people, organizations, and technologies that need to collaborate to effectively plan for emergencies. GAO did not independently verify state responses. In responding to GAO's survey, most SWICs reported not having a comprehensive emergency communications plans in place prior to PKEMRA's 2006 enactment. In particular, prior to the enactment of PKEMRA, only a few states had comprehensive emergency communications plans in place, but now all but one have such a plan. Most of the SWICs also reported that their statewide plans cover key elements, such as governance, standard operating procedures, and training and exercises, which are considered by DHS as the essential foundation for achieving the NECP goals.

GAO is making recommendations to DHS aimed at improving the ECPC's collaborative efforts, including defining its goals and tracking its recommendations. DHS concurred with the recommendations.

DHS OIG Reports

FEMA Was Generally Effective in Its Initial Response to the Severe Wildfires in California

Number: OIG-16-106-D
Date: 06/27/2016
Summary: For the most part, FEMA responded effectively to the 2015 Northern California wildfires. In evaluating FEMA's response to this disaster, we focused on answering the following questions:

1. What activities did FEMA perform before the major disaster declaration?
2. What were the most pressing challenges FEMA faced in this disaster?

3. What were the most significant resource shortfalls?
4. How did FEMA make disaster-sourcing decisions?
5. How well did FEMA coordinate its activities?

While FEMA successfully overcame most challenges that this disaster presented, we did observe one other matter that we reported on separately. Specifically, we observed instances where FEMA personnel did not properly safeguard Personally Identifiable Information according to Federal privacy and security standards. We determined that this occurred in part because FEMA's methods for training and promoting Privacy Awareness were not reliable. We discussed our observations with FEMA officials during our fieldwork and issued a separate management advisory report to inform FEMA of this issue. FEMA officials generally agreed with our findings and observations. Appendix B includes FEMA's written response in its entirety. Because we are making no recommendations, we consider this report closed.

FEMA's Initial Response to the 2015 Texas Spring Severe Storms and Flooding

Number: OIG-16-85-D
Date: 05/09/2016
Summary: FEMA's response to the severe storms and floods in Texas appeared effective. FEMA faced several significant challenges and resource shortages which include disaster reservist equipment shortage; availability and training; and timeliness of leasing the Joint Field Office. FEMA coordinated with State, local and other Federal agencies to provide disaster services. By December 15, 2015, FEMA—

- obligated $197 million dollars, including more than $66 million in Individual Assistance and approximately $37 million for Public Assistance programs;
- completed 29,036 housing inspections, 110 applicant briefings, and 394 kickoff meetings; and
- opened 53 centers throughout the State to assist disaster survivors.

In addition, by planning and deploying to the disaster within 9 days of the declaration, we proactively provided FEMA and State officials, along with potential Public Assistance applicants, relevant and accurate information on Federal regulations and our frequent audit findings. In coordination with our Office of Investigations, we also briefed local government officials and individual homeowners on the risks of contractor fraud related to debris removal and emergency services. DHS Office of Inspector General auditors and FEMA Region VI officials worked together to reconcile our audit results.

FEMA's Initial Response to the Severe Storms and Flooding in South Carolina

Number: OIG-16-53-D
Date: 03/21/2016
Summary: The Federal Emergency Management Agency (FEMA) responded effectively to the 2015 South Carolina storms and flooding. FEMA completed all Preliminary Damage Assessments

approximately two weeks after the declaration; overcame pressing challenges and sourcing decisions; and effectively coordinated its activities with Federal, State, and local partners.

In addition, by deploying to the disaster shortly after the declaration, we proactively provided FEMA and State officials, along with potential Public Assistance applicants, relevant and accurate information on our common findings. We emphasized the importance of proper accounting and procurement and retaining adequate support for expenses. Within 2 months of the disaster declaration, FEMA had registered over 90,000 disaster survivors under FEMA's Individual Assistance Program, approved $70 million in individual and household funds, completed 99 percent of housing inspections, opened 36 Disaster Recovery Centers, and completed 180 kickoff meetings.

FEMA officials generally agreed with our findings and observations. Because we are making no recommendations, we consider this report closed.

DHS' Ebola Response Needs Better Coordination, Training, and Execution

Number: OIG-16-18
Date: 01/06/2016
Summary: Although the Department responded quickly to implement domestic Ebola screening with the Department of Health and Human Services (HHS), it did not ensure sufficient coordination, adequate training, and consistent screening of people arriving at U.S. ports of entry. Coordination between DHS, HHS, and other DHS components was not sufficient to ensure all passengers received full screening. Components did not ensure all personnel received adequate training on the screening process or the use of certain protective equipment. Component personnel also did not always follow established Ebola procedures and ensure all identified passengers completed required screening. As a result, some passengers with potential risk of Ebola exposure may have entered the United States without having their temperatures taken or otherwise cleared by health professionals, and the DHS workforce performing the response was not always appropriately protected. The Department concurred with all 10 recommendations and has initiated corrective actions that should improve the effectiveness of the Department's response to Ebola when implemented.

Goal 5.4: Enable Rapid Recovery

GAO Reports

No GAO reports were available that aligned to this goal.

DHS OIG Reports

FEMA Miscalculated the 50 Percent Rule when Deciding to Replace School Buildings after the West, Texas Explosion

Number: OIG-16-132-D
Date: 09/09/2016
Summary: The massive West, Texas fertilizer plant explosion severely damaged the School District's buildings. With help from nearby school districts and local businesses, School District officials worked quickly to return students to classes within 5 days of the explosion.

The School District accounted for and expended FEMA grant funds according to Federal regulations and FEMA guidelines. However, FEMA Region VI officials made mistakes calculating the 50 Percent Rule it used to decide whether to replace, rather than repair, damaged buildings. Fortunately, these mistakes did not result in incorrect decisions.

In five audits spanning several FEMA Regional offices from 2012 and 2013, we identified over $100 million in ineligible costs stemming from mistakes FEMA made in applying the 50 Percent Rule. FEMA Headquarters recently issued policy clarification to help prevent improper replacement decisions, which, along with more detailed reviews, should help FEMA avoid future mistakes. FEMA officials agreed with our finding and recommendation. At the exit conference, FEMA provided sufficient evidence to resolve and close the recommendation. Therefore, we consider this audit closed.

FEMA Can Do More to Improve Public Assistance Grantees' and Subgrantees' Compliance with Federal Procurement Rules

Number: OIG-16-126-D
Date: 09/02/2016
Summary: The Federal Emergency Management Agency (FEMA) does not effectively enforce subgrantees' compliance with Federal procurement rules and has allowed the vast majority of procurement costs we questioned in our audits. Over a 6-year period ended September 30, 2014, our audits questioned $352.3 million in Public Assistance grant costs for noncompliance. FEMA officials subsequently ruled that $321.7 million, or 91.3 percent, of those costs were eligible.

We questioned these costs because Public Assistance subgrantees (local governments and nonprofit organizations) did not follow Federal rules in awarding contracts. They often failed to conduct full and open competition with contractors to lessen the risks of fraud, waste, and abuse. Many also failed to provide opportunities for disadvantaged firms such as minority firms and women's business enterprises to bid on work funded with Federal dollars as Congress intended.

Without consistent enforcement, FEMA's Public Assistance grantees and subgrantees have little incentive to comply with Federal regulations. And, because we are only able to audit a small fraction of FEMA's multibillion-dollar Public Assistance grant program per year, FEMA's allowance of ineligible contract costs may be much more widespread than our reports show.

Although we recognize FEMA has taken positive steps to lessen the risk of noncompliance with procurement requirements, we believe that additional corrective actions will lessen the risks to taxpayer funds invested in disaster relief. FEMA officials provided a written response to a draft of this report. In that response, FEMA officials generally concurred with the findings and recommendations in this report. FEMA's written response also included action plans for implementation of corrective actions.

FEMA Continues to Experience Challenges in Protecting Personally Identifiable Information at Disaster Recovery Centers

Number: OIG-16-102-D
Date: 06/09/2016
Summary: During our deployment to the 2015 California wildfire disaster, we observed that FEMA personnel at Disaster Recovery Centers did not properly safeguard PII, as Federal guidelines require. The mishandling of PII increases the risk of identity theft and can result in substantial harm, embarrassment, inconvenience, or unfairness to individuals. We also determined that some FEMA officials are not fully aware of Federal privacy standards. Moreover, FEMA management and trainers lack an effective method to track employee compliance with privacy training or to promote privacy awareness at disaster relief sites.

In May 2013, we reported similar deficiencies. As a result, FEMA officials stated that they would implement corrective actions, including conducting privacy compliance inspections at all disaster relief sites. However, FEMA officials at Disaster Recovery Centers for the 2015 California wildfire disaster were not aware of any privacy compliance inspections conducted at this disaster. While FEMA has made significant progress in developing a culture of privacy protection, it clearly needs to do more to safeguard private information at these sites. FEMA officials agreed with our findings and recommendations.

FEMA Has No Assurance that Only Designated Recipients Received $6.37 Million in Fuel

Number: OIG-16-04-D
Date: 11/02/15
Summary: FEMA has no assurance that mission-assigned fuel deliveries for New York went only to FEMA-designated recipients. We reviewed the $6.37 million FEMA paid the Defense Logistics Agency for 1.7 million gallons of fuel. However, of this amount, we found incomplete and questionable supporting documentation for $4.56 million in fuel deliveries. Therefore, we could not verify the eligibility of the recipients that received this fuel. In addition, the Defense Logistics Agency delivered $1.81 million of fuel to recipients outside the mission assignment's scope of work. As a result, FEMA cannot be sure that any of the fuel went to approved power restoration or emergency public transportation work in New York, as FEMA intended.

This occurred because FEMA did not comply with certain Federal regulations and internal control standards. When we ended field work, FEMA had recognized these challenges and was working to address them. For example, FEMA had started to develop procedures to account for large-scale,

disaster fuel support. FEMA also began efforts to improve its mission assignment process. FEMA concurred with all five recommendations.

FEMA Faces Challenges in Verifying Applicants' Insurance Policies for the Individuals and Households Program

Number: OIG-16-01-D
Date: 10/06/2016
Summary: Before authorizing Individuals and Households Program payments, FEMA does not verify the accuracy of applicants' "no insurance coverage" self-certifications. This condition exists because a reliable and comprehensive database does not exist for FEMA to verify the status of applicants' insurance coverage. Consequently, FEMA relies on self-certification and legal statements on the application to ensure accuracy of applicants' "no insurance coverage" information. FEMA is thereby exposing Federal disaster assistance funds to possible duplicate, improper, or fraudulent payments. We determined that FEMA paid approximately $250 million in homeowners' assistance to more than 29,000 Hurricane Sandy applicants who may have had private insurance.

Federal statutes require FEMA to develop a verification process for the Individuals and Households Program that includes a database for minimizing risks of making duplicate payments and payments for fraudulent claims. These statutes also prohibit FEMA from providing duplicate benefits to applicants. Therefore, FEMA should use every reasonable control possible to ensure that applicants provide truthful information and understand the consequences of making false statements on applications for Federal funds. FEMA also needs to use available resources to review possible cases of duplicate benefits for recoupment and continue to research options to develop or use an already established database to identify, at the time of application, whether applicants have private insurance coverage.

FEMA concurred with our three recommendations. FEMA acknowledges that insurance verification plays a key role in FEMA's timely and accurate delivery of emergency assistance. In an effort to enhance existing processes, FEMA has researched the potential use of private sector insurance-related databases to determine whether an applicant has homeowners insurance at the time of registration. A comprehensive database does not exist for FEMA to independently verify applicants' insurance coverage, which is an issue especially when applicants self-certify as having no insurance. FEMA will continue to research potential insurance database options, but until a comprehensive one is identified, insurance verification may remain a challenge for FEMA.

Table of Smaller Reports

Date	Number	Title
9/29/2016	OIG-16-143-D	FEMA Should Recover $25.4 Million in Grant Funds Awarded to Louisville, Mississippi, for an April 2014 Disaster
9/26/2016	OIG-16-140-D	FEMA Should Recover $9.9 Million of $36.6 Million Awarded to the Town of North Hempstead, New York, for Hurricane Sandy Damages
9/23/2016	OIG-16-137-D	City of Eureka, Missouri, Needs Additional Assistance and Monitoring to Ensure Proper Management of Its $1.5 Million FEMA Grant

Date	Number	Title
9/22/2016	OIG-16-136-D	Calaveras County, California, Needs Additional State and FEMA Assistance in Managing Its $10.8 Million FEMA Grant
9/19/2016	OIG-16-135-D	FEMA Should Recover $3.4 Million of the $3.5 Million Awarded to Hope Academy for Hurricane Katrina Damages
9/9/2016	OIG-16-133-D	Louisiana Should Provide the Ouachita Parish Police Jury Assistance in Managing FEMA Grant Funds
9/2/2016	OIG-16-125-D	Long Beach City School District in New York Generally Accounted For and Expended FEMA Public Assistance Funds Properly
9/1/2016	OIG-16-124-D	Nebraska Public Power District Properly Managed FEMA Grant Funds Awarded for May 2014 Storms
8/19/2016	OIG-16-122-D	Portland, Oregon, Has Adequate Policies, Procedures, and Business Practices to Manage Its FEMA Grant Funding
8/19/2016	OIG-16-121-D	Washington County, Florida, Effectively Managed FEMA Public Assistance Grant Funds Awarded for a July 2013 Flood
8/17/2016	OIG-16-120-D	Phelps County, Missouri, Needs Additional Assistance and Monitoring to Ensure Proper Management of Its $1.97 Million FEMA Grant
8/16/2016	OIG-16-119-D	FEMA Improperly Awarded $47.3 Million to the City of Louisville, Mississippi
8/16/2016	OIG-16-118-D	Wisner-Pilger Public Schools, Nebraska, Took Corrective Actions to Comply with Federal Grant Award Requirements
8/12/2016	OIG-16-117-D	Ocean County, New Jersey, Generally Accounted for and Expended FEMA Public Assistance Funds Properly
8/11/2016	OIG-16-116-D	City of Hazelwood, Missouri, Needs Additional Assistance and Monitoring to Ensure Proper Management of Its Federal Grant
8/10/2016	OIG-16-115-D	FEMA Should Suspend All Grant Payments on the $29.9 Million Coastal Retrofit Program Until Mississippi Can Properly Account for Federal Funds
8/2/2016	OIG-16-114-D	The Village Of Pilger, Nebraska, Took Corrective Actions to Comply with Federal Grant Award Requirements
7/15/2016	OIG-16-112-D	FEMA Should Recover $2.2 Million of $27.2 Million in Public Assistance Grant Funds Awarded to Nashville-Davidson County, Tennessee, for May 2010 Flood Emergency Work
7/7/2016	OIG-16-110-D	Minneapolis Park and Recreation Board, Minneapolis, Minnesota, Generally Accounted For and Expended FEMA Grant Funds Properly
6/30/2016	OIG-16-107-D	The Baldwin County Commission Effectively Managed FEMA Grant Funds Awarded for Damages from Spring 2014 Storms
6/9/2016	OIG-16-104-D	The Office of Community Development Paid Most Contractors in a Timely Manner for Hazard Mitigation Work on Louisiana Homes
6/9/2016	OIG-16-103-D	Lake County, California, Should Continue to Improve Procurement Policies, Procedures, and Practices
6/8/2016	OIG-16-99-D	FEMA and California Need to Assist the City of Berkeley to Improve the Management of a $12 Million FEMA Grant
6/8/2016	OIG-16-97-D	FEMA Should Recover $51.2 Million in Grant Funds Awarded to Cimarron Electric Cooperative, Kingfisher, Oklahoma
5/27/2016	OIG-16-94-D	FEMA Held Augusta-Richmond County, Georgia, Accountable for Not Complying with Federal Contracting Requirements when Managing a 2014 Public Assistance Disaster Grant
5/9/2016	OIG-16-86-D	The West School Administration Effectively Accounted for the FEMA Emergency Grant Funds Awarded for the West, Texas Fertilizer Plant Explosion
5/3/2016	OIG-16-78-D	Colorado Should Provide the City of Evans More Assistance in Managing FEMA Grant Funds
4/20/2016	OIG-16-67-D	Lyons and Colorado Officials Should Continue to Improve Management of $36 Million FEMA Grant

Date	Number	Title
4/20/2016	OIG-16-66-D	FEMA Should Disallow $1.30 Million of $2.58 Million in Public Assistance Grant Funds Awarded to the Municipality of Villalba, Puerto Rico, for Hurricane Irene Damages
4/12/2016	OIG-16-63-D	San Bernardino County, California, Generally Accounted for and Expended FEMA Public Assistance Funds Properly
4/6/2016	OIG-16-60-D	FEMA Should Recover $267,960 of $4.46 Million in Public Assistance Grant Funds Awarded to the Municipality of Jayuya, Puerto Rico, for Hurricane Irene Damages
3/21/2016	OIG-16-52-D	FEMA Should Recover $312,117 of $1.6 Million Grant Funds Awarded to the Pueblo of Jemez, New Mexico
3/2/2016	OIG-16-43-D	The Puerto Rico Electric Power Authority Effectively Managed FEMA Public Assistance Grant Funds Awarded for Hurricane Irene in August 2011
2/19/2016	OIG-16-42-D	Colorado Springs, Colorado, Has Adequate Policies, Procedures, and Business Practices to Effectively Manage Its FEMA Public Assistance Grant Funding
2/18/2016	OIG-16-40-D	Colorado Springs Utilities, Colorado, Has Adequate Policies, Procedures, and Business Practices to Effectively Manage Its FEMA Public Assistance Grant Funding
2/11/2016	OIG-16-38-D	Oakwood Healthcare System, Dearborn, Michigan, Needed Additional Assistance in Managing its FEMA Public Assistance Grant Funding
2/2/2016	OIG-16-36-D	The University of Wisconsin-Superior Effectively Managed FEMA Grant Funds Awarded for Severe Storms and Flooding in June 2012
2/2/2016	OIG-16-35-D	Jamestown, Colorado, Needs Additional Assistance and Monitoring to Ensure Proper Management of Its $10.4 Million FEMA Grant
1/29/2016	OIG-16-33-D	Boulder, Colorado, Has Adequate Policies, Procedures, and Business Practices to Manage Its FEMA Grant Funding
1/26/2016	OIG-16-24-D	FEMA Should Recover $1.2 Million of $10.1 Million in Grant Funds Awarded to Tuscaloosa, Alabama, for a 2011 Disaster
1/22/2016	OIG-16-23-D	FEMA Should Disallow $1.2 Million of $6.0 Million in Public Assistance Program Grant Funds Awarded to the City of San Diego, California
1/21/2016	OIG-16-22-D	The City of Austin, Texas, Has Adequate Policies and Procedures to Comply with FEMA Public Assistance Grant Requirements
1/21/2016	OIG-16-21-D	Longmont and Colorado Officials Should Continue to Improve Management of $55.1 Million FEMA Grant
12/17/2015	OIG-16-14	Lower Mississippi River Port-wide Strategic Security Council Did Not Always Properly Manage, Distribute, or Spend Port Security Grant Funds
12/10/2015	OIG-16-13	Oversight of the Colorado Emergency Management Performance Grant Program Needs Improvement
11/30/2015	OIG-16-12-D	FEMA The City of Birmingham, Alabama, Generally Managed FEMA Grant Funds for April 2011 Tornadoes and Severe Storms Properly
11/19/2015	OIG-16-09-D	FEMA Should Recover $505,549 of $3.3 Million in Public Assistance Grant Funds Awarded to DeKalb County, Georgia, for Damages from a September 2009 Flood
11/5/2015	OIG-16-05-D	FEMA's Plan to Provide Permanent or Semi-Permanent Housing to the Oglala Sioux Tribe of the Pine Ridge Indian Reservation in South Dakota

Mature and Strengthen Homeland Security

Goal: Integrate Intelligence, Information Sharing, and Operations

GAO Reports

No GAO reports were available that aligned to this goal.

DHS OIG Reports

Office of Intelligence and Analysis Can Improve Transparency and Privacy

Number: OIG-16-93
Date: 05/17/2016
Summary: I&A has made progress in developing a culture of privacy. Specifically, I&A has centralized the oversight of privacy and civil liberties and has been working to ensure that it meets the requirements of pertinent legislation, regulations, directives, and guidance. I&A conducted specialized onboarding and advanced training that address safeguards for privacy and civil liberties in its intelligence processes. In addition, I&A designed intelligence oversight reviews to ensure that its employees observe the required safeguards.

However, I&A has faced challenges because it did not place priority on institutionalizing other capabilities and processes to ensure timely and complete compliance with requirements regarding privacy and intelligence information. Specifically:

- I&A has not responded timely to requests for agency transparency under the Freedom of Information Act, potentially creating financial liabilities.
- I&A continuity capabilities have not had an adequate oversight structure, risking the loss of essential records and intelligence information in an emergency.
- I&A has not implemented an infrastructure for risk assessment and end-to-end monitoring of high-impact solicitations and contracts that would ensure safeguards for sensitive data and systems throughout the acquisition processes.

I&A concurred with all six recommendations.

Evaluation of DHS' Information Security Program for Fiscal Year 2015

Number: OIG-16-08
Date: 01/5/2016
Summary: DHS has taken actions to strengthen its information security program. For example, DHS developed and implemented the Fiscal Year 2015 Information Security Performance Plan to define the performance requirements, priorities, and overall goals of the Department. DHS has also taken steps to address the President's cybersecurity priorities, such as Information Security Continuous Monitoring; Identity, Credential, and Access Management; and anti-phishing and malware defense.

Nonetheless, the Department must ensure compliance with information security requirements in other areas. For example, DHS did not include classified systems information in its monthly information security scorecard or its Federal Information Security Modernization Act of 2014 reporting submission to the Office of Management and Budget. Contrary to the Under Secretary's guidance, the United States Coast Guard (USCG) did not report its personal identity verification card implementation data to the Department. We also identified inaccurate or incomplete data in DHS' enterprise management systems.

Further, Components did not maintain their information security programs on a year-round, continuous basis or perform weakness remediation reviews as required. Components operated 220 "sensitive but unclassified," "Secret," and "Top Secret" systems with expired authorities to operate. We also identified deficiencies related to plans of action and milestones, configuration management, and continuous monitoring. Without addressing these deficiencies, the Department cannot ensure that its systems are properly secured to protect sensitive information stored and processed in them. We made six recommendations to the Chief Information Security Officer. The Department concurred with five recommendations.

Goal: Enhance Partnerships and Outreach

GAO Reports

No GAO reports were available that aligned to this goal.

DHS OIG Reports

No OIG reports were available that aligned to this goal.

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

GAO Reports

No GAO reports were available that aligned to this goal.

DHS OIG Reports

No OIG reports were available that aligned to this goal.

Goal: Conduct Homeland Security Research and Development

GAO Reports

No GAO reports were available that aligned to this goal.

DHS OIG Reports

No OIG reports were available that aligned to this goal.

Goal: Ensure Readiness of Frontline Operators and First Responders

GAO Reports

No GAO reports were available that aligned to this goal.

DHS OIG Reports

No OIG reports were available that aligned to this goal.

Goal: Strengthen Service Delivery and Manage DHS Resources

GAO Reports

Federal Real Property: Efforts Made, but Challenges Remain in Reducing Unneeded Facilities

Number: GAO-16-869T
Date: 09/23/2016
Summary: Since 2012, the administration has taken steps to reform real property management and address the long-standing challenge of reducing excess and underutilized property. For example, in 2015, the Office of Management and Budget (OMB) issued government-wide guidance—the National Strategy for the Efficient Use of Real Property—which GAO found in 2016 could help agencies strategically manage real property.

However, GAO's work has found that significant challenges persist in managing real property in general and excess and underutilized property in particular. They include:

- a lack of reliable data with which to measure the extent of the problem,
- a complex disposal process,
- costly environmental requirements,
- competing stakeholder interests, and
- limited accessibility of some federal properties.

Properties in the Washington, D.C., area such as the Cotton Annex building, vacant General Services Administration (GSA) warehouses, and buildings on the St. Elizabeths campus (pictured below) illustrate the challenges for disposal and re-utilization of vacant federal buildings. For example, GAO found in 2014 that real property data indicated some GSA warehouses were utilized when they had been vacant for as long as 10 years.

In addition to the steps already taken by the administration, further action by federal agencies to implement GAO's previous recommendations could help to address some of these challenges. For example, GAO has made recommendations to GSA and other federal agencies that, if implemented, would increase the federal government's capacity to manage its portfolio and document the progress of reform efforts. GAO highlighted its highest priority open recommendations to GSA in an August 2016 letter to GSA. Among those are three recommendations related to excess and underutilized property, including a recommendation to assess the reliability of data collected and entered into GSA's Federal Real Property Profile database by individual federal agencies. Additionally, real property reform bills that could address the long-standing problem of federal excess and underutilized property have been introduced in Congress. Specifically, two bills have been passed by the House of Representatives in 2016, but neither has been enacted yet.

DHS Management: Enhanced Oversight Could Better Ensure Programs Receiving Fees and Other Collections Use Funds Efficiently

Number: GAO-16-443
Date: 07/21/2016
Summary: The Department of Homeland Security (DHS) received $15 billion in fees and other collections across 38 programs in fiscal year 2014 that help fund homeland security functions, such as the screening and inspection of persons and goods entering the United States. Our analysis of DHS collections and cost data showed that 14 of the 38 programs receiving fees and other collections in fiscal year 2014 collected amounts that fully covered identified program costs. Of the remaining 24 programs, collections for 20 programs partially covered identified program costs, and DHS did not provide cost data, or we determined such data may not be reliable, for 4 programs. DHS components have taken action to address the estimated $6 billion difference between collections and identified program costs, with 6 programs comprising about 85 percent of the difference. However, components did not document processes for managing differences and making decisions on how to address the estimated $726 million difference across the 10 remaining programs. Such documentation of processes and decisions could help improve transparency and accountability over cost recovery efforts.

DHS components have processes in place to manage unobligated balances carried over across fiscal years for 25 programs, with such balances totaling $2.6 billion at fiscal year-end 2014. These processes generally focused on ensuring continuity of program operations rather than efficiently using funds. For example, while components established targets for minimum balances for 21 of these 25 programs, none of the components established processes and related maximum targets to manage excessive unobligated carryover balances. Establishing such management processes and targets for minimum and maximum balances would enable components to show that management actions will be sufficient and appropriate to ensure the efficient use of funds—such as the Immigration Examinations Fee Account, which had an approximately $983 million unobligated balance as of fiscal year end 2014, and the User Fee Facility program account for small airports which has an unobligated balance of $14 million that has exceeded 100 percent of total operating costs each year from fiscal year 2010 through fiscal year 2014.

DHS does not ensure that all components review their programs or monitor component actions to address management and operational deficiencies identified in those reviews. GAO found that three of the seven DHS components that have fee or other collection programs did not conduct such reviews for 6 of their programs, and that components had not taken recommended actions to address 9 of 20 deficiencies identified through program reviews as of fiscal year-end 2014. Further, DHS did not report the extent to which components are conducting such reviews or any proposals to address identified management and operational deficiencies. DHS oversight to ensure that components complete these reviews and report the results for all programs would enable Congress and others to receive information necessary to better ensure that fee and other collection programs are operating effectively and efficiently.

Federal Real Property: Observations on GSA's Canceled Swap Exchange Involving Buildings in the Federal Triangle South Area

Number: GAO-16-571R
Date: 06/16/16
Summary: In 2012, the General Services Administration (GSA) began exploring a project, called a "swap exchange," to exchange up to five office buildings located in the Federal Triangle South area of Washington, D.C., to finance construction services at GSA headquarters and other federal properties. The purpose of the exchange was to dispose of excess federal property while providing over 11,000 federal employees with improved office spaces. Informed by the responses from private real estate investors about their interests in this area, GSA subsequently focused the project on two buildings—the GSA's Regional Office Building (ROB) and the Department of Agriculture's Cotton Annex—in order to reduce some associated risks and facilitate a more manageable swap exchange. For example, five of nine respondents to a request for information noted the complexities of exchanging all five buildings in one project and one respondent suggested that GSA divide the project into a series of smaller transactions.

After evaluating proposals submitted in 2015 by three qualified investors, GSA canceled the project and concluded in its February 18, 2016 memorandum on the decision that private investors' valuations for these two buildings fell short of the government's estimated value. GAO independently analyzed the proposals and found that qualified investors' proposed values for the GSA ROB and the Cotton Annex were significantly less than those contained in an independent appraisal that GSA had obtained. These differences were due, in part, to the assumptions and methodologies used to make the GSA's and investors' valuations.

According to GSA officials, their experience with the canceled project will help guide future efforts. For example, GSA officials said that they plan to improve the appraisal process for buildings involved in swap exchanges by: (a) informing appraisers of the swap exchange's goals, objectives, and processes; (b) allowing appraisers to consider a range of values for uncertainties related to zoning and other economic assumptions; and (c) encouraging appraisers, when appropriate, to develop methodologies that take into consideration the size and complexity of proposed swap exchanges.

Managing for Results: Agencies Need to Fully Identify and Report Major Management Challenges and Actions to Resolve them in their Agency Performance Plans

Number: GAO-16-510
Date: 06/15/2016
Summary: The GPRA Modernization Act of 2010 (GPRAMA) requires agencies to describe their major management challenges and identify associated performance information in their agency performance plans (APP). GAO found, however, that 14 of 24 agencies reviewed did not describe their major management challenges in their APPs as required. This is, in part, because the Office of Management and Budget's (OMB) guidance is not clear that major management challenges should be identified in the APP. GPRAMA also requires agencies to develop and report performance

information–specifically performance goals, measures, milestones, planned actions, and an agency official responsible–needed to resolve the issue. However, GAO found that 22 of the 24 agencies reviewed did not report complete performance information for each of their major management challenges. Again, this may be in part because OMB's guidance is unclear. As a result, it was not always transparent what these agencies considered to be their major management challenges or how they planned to resolve these challenges. GAO also found that the number of major management challenges reported by these agencies ranged from none (Nuclear Regulatory Commission) to 17 (Department of Defense) with most having 5 or more. GAO found there were generally seven management functions that were most frequently cited as major management challenges across these 24 agencies: 1) acquisition and procurement, 2) contract management and contractor oversight, 3) cybersecurity, 4) financial management, 5) human capital management, 6) addressing improper payments, and 7) real property management.

GAO selected illustrative examples from the Environmental Protection Agency (EPA), Department of Homeland Security (DHS), and the National Aeronautics and Space Administration (NASA) to demonstrate actions agency officials took to help address an area that they determined to be a management challenge and was also one of GAO's high-risk areas. For example, DHS began implementing an action plan with milestones and performance measures to strengthen its management functions which is also a high risk issue area; and NASA implemented key components of an action plan including instituting new tools aimed at providing increased insight into project performance over its acquisition management high risk area. While more work remains for these three agencies, the actions taken to date show progress and align with GPRAMA requirements that challenges should also include performance information.

Information Technology: Federal Agencies Need to Address Aging Legacy Systems

Number: GAO-16-468
Date: 05/25/2016
Summary: The federal government spent about 75 percent of the total amount budgeted for information technology (IT) for fiscal year 2015 on operations and maintenance (O&M) investments. Such spending has increased over the past 7 fiscal years, which has resulted in a $7.3 billion decline from fiscal years 2010 to 2017 in development, modernization, and enhancement activities.

Specifically, 5,233 of the government's approximately 7,000 IT investments are spending all of their funds on O&M activities. Moreover, the Office of Management and Budget (OMB) has directed agencies to identify IT O&M expenditures known as non-provisioned services that do not use solutions often viewed as more efficient, such as cloud computing and shared services. Agencies reported planned spending of nearly $55 billion on such non-provisioned IT in fiscal year 2015. OMB has developed a metric for agencies to measure their spending on services such as cloud computing and shared services, but has not identified an associated goal. Thus, agencies may be limited in their ability to evaluate progress.

Many O&M investments in GAO's review were identified as moderate to high risk by agency CIOs, and agencies did not consistently perform required analysis of these at-risk investments. Further,

several of the at-risk investments did not have plans to be retired or modernized. Until agencies fully review their at-risk investments, the government's oversight of such investments will be limited and its spending could be wasteful.

Federal legacy IT investments are becoming increasingly obsolete: many use outdated software languages and hardware parts that are unsupported. Agencies reported using several systems that have components that are, in some cases, at least 50 years old. For example, Department of Defense uses 8-inch floppy disks in a legacy system that coordinates the operational functions of the nation's nuclear forces. In addition, Department of the Treasury uses assembly language code—a computer language initially used in the 1950s and typically tied to the hardware for which it was developed. OMB recently began an initiative to modernize, retire, and replace the federal government's legacy IT systems. As part of this, OMB drafted guidance requiring agencies to identify, prioritize, and plan to modernize legacy systems. However, until this policy is finalized and fully executed, the government runs the risk of maintaining systems that have outlived their effectiveness. The following table provides examples of legacy systems across the federal government that agencies report are 30 years or older and use obsolete software or hardware, and identifies those that do not have specific plans with time frames to modernize or replace these investments.

Quadrennial Homeland Security Review: Improved Risk Analysis and Stakeholder Consultations Could Enhance Future Reviews

Number: GAO-16-371
Date: 04/15/2016
Summary: The Department of Homeland Security (DHS) assessed risk for the second Quadrennial Homeland Security Review (QHSR) and considered threats, vulnerabilities, and consequences; however, DHS did not document how its various analyses were synthesized to generate results, thus limiting the reproducibility and defensibility of the results. Without sufficient documentation, the QHSR risk results cannot easily be validated or the assumptions tested, hindering DHS's ability to improve future assessments. In addition, the QHSR describes homeland security hazards, but does not rank those hazards or provide prioritized strategies to address them. Comparing and prioritizing risks helps identify where risk mitigation is most needed and helps justify cost-effective risk management options. Without determining prioritized risk outcomes, DHS is missing an opportunity to more efficiently mitigate risk or identify the resources required for addressing different levels and types of risks.

The President's fiscal years 2015 and 2016 budget requests for DHS were generally presented in alignment with the QHSR. However, DHS has faced challenges accounting for its spending by mission, which it is taking actions to address, such as developing a new common appropriation structure to better link the department's funding request to the execution of its missions. DHS also developed performance measures for all of the QHSR mission areas.

DHS expanded its stakeholder outreach efforts, but 43 of 61 stakeholders who provided narrative responses to one question in GAO's survey stated that collaboration with stakeholders could be improved. For example, one respondent reported that stakeholders were asked to react to information provided by DHS rather than assist in formulating the QHSR approach and execution. DHS officials reported being limited by staff, time, and other constraints, and thus directed stakeholders to provide feedback via various web-based forums. Although the online forums

allowed DHS to reach 2,000 representatives during its 2014 QHSR development process, DHS's QHSR After Action Report noted that the tools were used to validate study findings instead of informing them. Without fostering interactive communication, DHS may miss opportunities to incorporate stakeholder perspectives from the entire homeland security enterprise and thereby may not have fully informed the QHSR effort.

Administrative Leave: Evaluation of DHS's New Policy Can Help Identify Progress toward Reducing Leave Use

Number: GAO-16-342
Date: 03/23/2016
Summary: Between fiscal years 2011 and 2015, 116 Department of Homeland Security (DHS) employees were on administrative leave for personnel matters for 1 year or more, with a total estimated salary cost of $19.8 million for this period. Of these 116 employees on administrative leave:

- 69 employees (59 percent) were for matters related to misconduct allegations,
- 28 employees (24 percent) were for matters related to fitness for duty issues, and
- 19 employees (or 16 percent) were for matters related to security clearance investigations.

As of September 30, 2015, DHS reported that of these 116 employees:

- 68 employees (59 percent) were separated from the agency,
- 32 employees (28 percent) were back on duty,
- 2 employees (2 percent) were on indefinite suspension, and
- 14 employees (12 percent) remained on administrative leave.

Several factors can contribute to the length of time an employee is on administrative leave for personnel matters, such as certain legal procedural steps that must be completed before suspending or removing an employee, or time needed for completing investigations. For example, in one particularly long and complex misconduct investigation, an employee was on administrative leave for over 2 years while investigating officials conducted over 50 interviews abroad.

In September 2015, DHS issued an administrative leave policy to ensure proper and limited use of administrative leave across the department. The policy clarifies when such leave is proper, elevates the level of management approval needed for longer periods of leave, and requires quarterly reporting of leave use to component heads and the Chief Human Capital Officer. Component policies and procedures varied prior to the DHS policy; however, component officials stated they would make changes needed to comply with the new policy. Federal internal control standards call for agencies to conduct routine monitoring and separate evaluations to ensure agency controls are effective, and to share their results. While the quarterly reports required under DHS's policy provide routine monitoring information, the policy does not address how DHS will evaluate the effectiveness of the policy and related procedures or how DHS will share lessons learned. DHS officials said they plan to learn from reviewing quarterly reports, but agreed evaluations could be valuable in assessing policy effectiveness. Evaluations of DHS's administrative leave policy can help the department identify effective practices for managing administrative leave, as well as

agency inefficiencies that increase the time employees spend on such leave. Sharing evaluation results with components may help ensure DHS's administrative leave policy and procedures are effective, and are achieving the intended result of reducing leave use.

Department of Homeland Security: Progress Made, but Work Remains in Strengthening Acquisition and Other Management Functions

Number: GAO-16-507T
Date: 03/16/2016
Summary: The Department of Homeland Security's (DHS) efforts to strengthen and integrate its management functions have resulted in it meeting three and partially meeting two of GAO's criteria for removal from the high-risk list.

For example, DHS has established a plan for addressing the high-risk area and a framework for monitoring its progress in implementing the plan. However, DHS needs to show additional results in other areas, including demonstrating the ability to achieve sustained progress across 30 outcomes that GAO identified and DHS agreed were needed to address the high-risk area. As of March 2016, DHS had fully addressed 10 of these outcomes but work remained in 20.

GAO has reported on DHS's acquisition management for over 10 years. The department has struggled to effectively manage its major programs, including ensuring that all major acquisitions had approved baselines and that they were affordable. GAO has noted significant progress in recent reviews. This progress is largely attributable to sustained senior leadership attention.

To ensure that recent efforts are sustained, the department must continue to implement its sound acquisition policy consistently and effectively across all components. GAO has made numerous recommendations in this regard, which DHS has concurred with and is taking actions to implement.

Federal Vehicles: Composition and Management of Agency Fleets

Number: GAO-16-455T
Date: 02/26/2016
Summary: The federal vehicle fleet consists of dozens of agencies' fleets that range in size from just a few vehicles to more than 200,000. The vehicles agencies use to carry out these missions also vary and include passenger cars and trucks and special purpose vehicles (e.g., ambulances and buses.) In fiscal year 2014, the most recently available data, seven agencies owned or leased approximately 78 percent of non-tactical federal vehicles. Approximately one-third of these vehicles belonged to the U.S. Postal Service, and approximately 45 percent were owned or leased by six other agencies--the U.S. Air Force, U.S. Army, Department of Homeland Security (DHS), the Department of Justice, the U.S. Navy, and the Department of Agriculture. As GAO reported in January 2016, fleet management is generally decentralized, as agencies are responsible for managing their vehicles in a manner that allows them to fulfill their missions and meet various federal requirements. Among other things, agencies determine the number and type of vehicles they need to own or lease and also determine the criteria used to determine if the vehicle is utilized. For example, agencies use criteria such as annual miles traveled or days used per month. For those vehicles that do not meet the utilization criteria, Federal Property Management Regulations allow

agencies to individually justify a vehicle. According to General Services Administration (GSA) officials, GSA provides guidance to assist agencies, such as vehicle purchasing and maintenance services, but does not have oversight responsibility. In January 2016, GAO reported on the vehicle utilization processes in 5 agencies and found that 4 agencies could not readily provide justifications for leased vehicles that did not meet the agency's utilization criteria. GAO also found 2 agencies that cumulatively retained over 500 vehicles that did not meet the agency's utilization criteria or have another form of justification. It is critical that agencies have procedures and data that provide assurance they are using their fleets to meet missions in the most cost-effective way possible.

Homeland Security: Oversight of Neglected Human Resources Information Technology Investment Is Needed

Number: GAO-16-253
Date: 02/11/2016
Summary: The Department of Homeland Security (DHS) has made very little progress in implementing its Human Resources Information Technology (HRIT) investment in the last several years. This investment includes 15 improvement opportunities; as of November 2015, DHS had fully implemented only 1.

HRIT's limited progress was due in part to the lack of involvement of its executive steering committee—the investment's core oversight and advisory body—which was minimally involved with HRIT, such as meeting only one time during a nearly 2-year period when major problems, including schedule delays, were occurring. As a result, key governance activities, such as approval of HRIT's operational plan, were not completed. Officials acknowledged that HRIT should be re-evaluated and took early steps to do so (i.e., meeting to discuss the need to re-evaluate); however, specific actions and time frames have not been determined. Until DHS takes key actions to re-evaluate and manage this neglected investment, it is unknown when its human capital weaknesses will be addressed.

Coast Guard Acquisitions: Enhanced Oversight of Testing Could Benefit National Security Cutter Program and Future DHS Acquisitions

Number: GAO-16-314T
Date: 02/03/2016
Summary: In January 2016, GAO reported that the Navy's Commander, Operational Test and Evaluation Force conducted the initial testing on the National Security Cutter (NSC) in spring 2014, when three of the cutters were already operational. The Navy deemed the NSC operationally effective and suitable. At the same time however, the testing revealed some major deficiencies. Two metrics used to assess an asset in testing are key performance parameters (KPP) and critical operational issues (COI). The NSC met 18 of 19 COIs and 12 of its 19 KPPs. Navy testers found 10 major deficiencies that varied in terms of their effect on the NSC program, including 4 deficiencies related to the NSC's weapon systems and 1 for its cutter boats. The Coast Guard plans to correct most of the NSC's major deficiencies.

Also, as GAO reported, following initial testing, a Department of Homeland Security (DHS) acquisition review board approved the NSC program for full rate production in October 2014. The Coast Guard plans to begin follow-on testing in fall 2016. DHS acquisition guidance does not specify the timing of follow-on testing for its programs or any actions program offices should take in response to the findings of follow-on testing. As a result, future DHS acquisitions risk fielding assets without knowing the full capabilities, as was the case with the NSC.

GAO also found that problems discovered outside of testing are preventing the Coast Guard from operating fully capable NSCs. By the time of initial testing, the Coast Guard had nearly 4 years' experience operating NSCs and has encountered issues that require retrofits. In order to minimize cost increases for some changes, the Coast Guard plans to maintain the original equipment for the production of the remaining NSCs and conduct retrofits after accepting delivery. In some instances, replacement equipment is still in the prototype phase. The identified problems will continue to affect the NSC until retrofits are implemented.

GAO has observed, based on prior work reviewing the Coast Guard's ongoing Fast Response Cutter program and plans for its upcoming Offshore Patrol Cutter program, that the Coast Guard has matured its acquisition process. The process to date reflects some lessons learned from the NSC acquisition, for example in the areas of competition and the schedule for initial testing. Furthermore, as the $12 billion Offshore Patrol Cutter program moves forward, it may have opportunities to further incorporate some best practices that GAO has highlighted in May 2009 (GAO-09-322) and March 2013 (GAO-13-325) on other shipbuilding work. For example, before a contract is signed, best practices call for a full understanding of the effort needed to design and construct the ship to be reached, enabling commercial buyers and shipbuilders to sign a contract that fixes the price, delivery date, and ship performance parameters.

Federal Acquisitions: Use of 'Other Transaction' Agreements Limited and Mostly for Research and Development Activities

Number: GAO-16-209
Date: 01/07/2016
Summary: Congress has authorized 11 federal agencies to use other transaction agreements—which generally do not follow a standard format or include terms and conditions required in traditional mechanisms, such as contracts or grants—to help meet project requirements and mission needs. The National Aeronautics and Space Administration (NASA) first received this authority in 1958. Over the next several decades, five additional federal departments were given this authority—Defense (DOD), Energy (DOE), Health and Human Services (HHS), Homeland Security (DHS), and Transportation (DOT). Congress also granted authority to five agencies within these departments, including DOT's Federal Aviation Administration and DHS's Transportation Security Administration (TSA). The statutory authorities for most agencies include some limitations on the use of their agreements, although the extent and type of limitations vary. For example, DOT's authority limits use of other transaction agreements to research, development, and demonstration (RD&D) projects that focus on public transportation. Ten of the 11 agencies have issued guidance to implement their authority. The last agency—the National Institutes of Health (NIH)—is in the process of developing guidance.

Most agencies cited flexibility as a primary reason for their use of other transaction agreements, and used agreements mostly for RD&D activities. Officials from 7 agencies told GAO the authority allowed them to develop customized agreements that addressed concerns over requirements in traditional mechanisms that some companies viewed as potential obstacles to doing business with a federal agency. This flexibility allowed agencies to address concerns regarding intellectual property and cost accounting provisions that would otherwise need to be included when using traditional mechanisms, such as contracts. In addition, other transaction agreements allowed some agencies to tailor other terms and conditions of agreements as needed when working with other entities. Most agencies—9 of the 11—used other transaction agreements for RD&D activities for a range of projects from medical research to energy development research. Two of the 9 agencies—DOD and DHS—also used other transaction agreements for prototype activities. Three agencies, including TSA and NASA, used other transaction agreements for activities not related to RD&D or prototype development, including airport security and education and outreach.

Other transaction agreements were a small proportion of most agencies' contracting and financial assistance activities for fiscal years 2010 through 2014. Compared to traditional mechanisms, most agencies used other transaction agreements sparingly, according to officials. Most agencies had a small number of other transaction agreements—75 or fewer—in fiscal year 2010, and the number of agreements generally remained low by the end of fiscal year 2014. Officials cited budgetary and other reasons for this trend. In contrast, two agencies that used other transaction agreements for activities other than RD&D and prototypes—TSA and NASA—had larger numbers of agreements. In fiscal year 2010, TSA and NASA had about 400 and 2,220 agreements, respectively. By the end of fiscal year 2014, these agencies had increased their use to about 640 and 3,220 agreements, respectively.

Strategic Sourcing: Opportunities Exist to Better Manage Information Technology Services Spending

Number: GAO-15-549
Date: 09/22/2015
Summary: Efforts by the Departments of Defense (DOD), Homeland Security (DHS), and the National Aeronautics and Space Administration (NASA) to strategically manage spending for information technology (IT) services, such as software design and development, have improved in recent years. Each of the agencies GAO reviewed has designated officials responsible for strategic sourcing and created offices to identify and implement strategic sourcing opportunities, including those specific to IT services. Most of these agencies' IT services spending, however, continues to be obligated through hundreds of potentially duplicative contracts that diminish the government's buying power. These agencies managed between 10 and 44 percent of their IT services spending through preferred strategic sourcing contracts in fiscal year 2013. In contrast, GAO previously reported that leading companies generally strategically managed about 90 percent of their procurement spending, including services.

Further, most of these agencies' efforts to strategically source IT services have not followed leading commercial practices, such as clearly defining the roles and responsibilities of the offices responsible for strategic sourcing; conducting an enterprise-wide spend analysis; monitoring the spending going through the agencies' strategic sourcing contract vehicles; or establishing savings

goals and metrics. As a result, the agencies are missing opportunities to leverage their buying power and more effectively acquire IT services.

Contracting officials from the agencies GAO reviewed generally had limited insights into the labor rates paid for similar IT services. GAO's analysis of 30 contract actions for similar IT services in fiscal year 2013 found that the agencies paid widely varying labor rates for similar services with the same contractors. The average difference between the lowest and highest labor rate for the categories GAO reviewed was 62 percent, in part due to geographic or work location, unique security, education or skill requirements, and the contractor unit performing the work. Further, for the 30 contract actions for IT services that GAO reviewed, the two contractors proposed more than 117 discrete labor categories—some with multiple variations—which complicated efforts to compare labor rates. Prior GAO reports on leading commercial practices have noted that companies use standardized labor categories for IT services to enable comparison of labor rates and ultimately realize cost savings. Several government-wide and agency-specific efforts to address aspects of these challenges, including providing tools to assess labor rate variations or streamlining labor categories, are under development or in their early implementation stages.

National Protection and Programs Directorate: Factors to Consider when Reorganizing

Number: GAO-16-140T
Date: 10/07/2015
Summary: GAO's prior work includes four areas for agency officials' consideration when evaluating or implementing a reorganization or transformation.

First, GAO reported in May 2012 on key questions to consider when evaluating an organizational change that involves consolidation, such as what are the goals of the consolidation and how have stakeholders been involved in the decision-making? For reorganization implementation, GAO's prior findings reported in July 2003 include lessons learned from the experiences of large private and public sector organizations. The resulting practices GAO developed include ensuring that top leadership drives the transformation and establishing a communication strategy to create shared expectations and report related progress.

Second, GAO reported in March 2012 that successful government reorganizations balanced executive and legislative roles. Specifically, GAO reported that all key players should be engaged in discussions about reorganizing government: the President, Congress, and other parties with vested interests. It is important that consensus is obtained on identified problems and needs, and that the solutions the U.S. government legislates and implements can effectively remedy the problems the nation faces in a timely manner. Fixing the wrong problems, or even worse, fixing the right problems poorly, could cause more harm than good.

Third, GAO's applicable high-risk work identifies areas that agency officials should consider as part of a reorganization. For example, one high-risk area is securing cyber critical infrastructure and federal information systems and protecting the privacy of personally identifiable information. Specifically, safeguarding the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—is a continuing concern cited in GAO's 2015 High Risk Series Update report. Given the National Protection and Programs Directorate's (NPPD) current

cybersecurity activities, addressing these concerns in any reorganization effort would be critical. For example, NPPD conducts analysis of cyber and physical critical infrastructure interdependencies and the impact of a cyber threat or incident to the Nation's critical infrastructure. Sustained attention to this function is vitally important.

Fourth, GAO has identified areas where agencies may be able to achieve greater efficiency or effectiveness by reducing programmatic duplication, overlap, and fragmentation. Since 2011, GAO has reported annually on this topic. Several of its findings in the reports relate to DHS and NPPD activities. For example, in 2015 GAO reiterated a September 2014 recommendation that DHS should mitigate potential duplication or gaps by consistently capturing and maintaining data from overlapping vulnerability assessments of critical infrastructure and improving data sharing and coordination among the offices and components involved with these assessments, of which NPPD is one. DHS agreed with the recommendation. Attention to potential programmatic overlap, duplication, and fragmentation during an NPPD reorganization could improve the agency's overall efficiency.

DHS OIG Reports

DHS' Progress in Implementing the Federal Information Technology Acquisition Reform Act

Number: OIG-16-138
Date: 10/21/2016
Summary: The Department of Homeland Security (DHS) reported substantial progress implementing the Federal Information Technology Acquisition Reform Act (FITARA) to improve department-wide IT management and oversight. As of April 2016, DHS stated it had implemented 11 of the 17 required FITARA elements to enhance the Chief Information Officer's (CIO) budget, acquisition, and organizational authority. Milestones have been established to fulfill the remaining six elements by March 2018. The reported progress was largely due to the focused efforts of CIO office personnel to establish a FITARA Implementation Team and ensure DHS-wide collaboration. Such actions have resulted in department-wide IT management enhancements and policy revisions, although the outcome of these actions could not yet be measured at the time of our review.

The Department must take additional steps to improve IT investment transparency, risk management, and review and reporting processes in line with FITARA. The CIO office has implemented several key enhancements, such as updating the agency-wide IT portfolio review process. However, other requirements such as reporting on the use of incremental development and conducting program reviews of high-risk investments were not fully met. These shortfalls were due, in part, to incomplete departmental processes to ensure compliance. Until these requirements are fully implemented, DHS will be challenged to ensure accurate reporting on adoption of incremental development and timely reviews of its high-risk IT investments.

DHS Has Not Trained Classified Network Users on the Classification Management Tool

Number: OIG-16-141
Date: 09/26/2016
Summary: In 2014, DHS deployed a new classification management tool (CMT) to help users properly mark classified documents and emails. However, the Department has not trained employees on using the CMT. As a result, employees reported they had difficulty using the tool when marking and sending classified emails. We also reviewed 269 classified documents and identified 48 classification marking errors, which resulted in an error rate similar to the rate we identified during our 2013 document review. Training, as well as using the CMT when creating these documents, would help employees identify and correct many of these errors. Without such training, DHS will not realize the full potential of the CMT.

Review of DHS' Information Security Program for Intelligence Systems for Fiscal Year 2016

Number: OIG-16-131
Date: 09/09/2016
Summary: We evaluated the Department of Homeland Security (DHS) enterprise-wide security program for Top Secret/Sensitive Compartmented Information intelligence systems. We assessed DHS programs for continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plans of actions and milestones, remote access management, contingency planning, and contractor systems. This report will be issued to the Office of the Inspector General of the Intelligence Community, in accordance with reporting instructions dated May 10, 2016.

Pursuant to the Federal Information Security Modernization Act of 2014, we reviewed the Department's security program, including its policies, procedures, and system security controls for the enterprise-wide intelligence system. Since our FY 2015 evaluation, the Office of Intelligence and Analysis has continued to provide effective oversight of the department-wide system and has implemented programs to monitor ongoing security practices. In addition, Intelligence and Analysis has relocated its intelligence system to a DHS data center to improve network resiliency and support.

The United States Coast Guard (USCG) has migrated all of its sites that process Top Secret/Sensitive Compartmented Information to the Department of Defense Intelligence Information System owned by the Defense Intelligence Agency. However, USCG must continue to work with the Defense Intelligence Agency to clearly identify agency oversight responsibilities for the Department of Defense Intelligence Information System enclaves that support USCG's intelligence operations.

We conducted our fieldwork between March and August 2016. This report does not contain any recommendations.

Fiscal Year 2015 Risk Assessment of the DHS Bank Card Program Indicates Moderate Risk

Number: OIG-16-129
Date: 09/02/1994
Summary: In fiscal year 2015, the Department spent almost $1 billion in purchase and travel card transactions.

Although the Department has established internal controls for its charge card programs, the components did not always follow DHS' required procedures for credit card use. In addition, they did not always have their own procedures in place to supplement those developed by DHS.

The Department remains at a moderate level of risk for its purchase and travel card programs. As a result, there remains a risk that DHS' internal controls will not prevent illegal, improper, or erroneous purchases and payments.

CBP's Office of Professional Responsibility's Privacy Policies and Practices

Number: OIG-16-123
Date: 08/29/2016
Summary: While investigating two individuals who trained people on counter-measure techniques for passing polygraph exams, CBP OPR collected, enhanced, stored, and shared sensitive PII. In one investigation, after confirming the individuals had extensive contact with the subject of the investigation, CBP OPR shared the sensitive PII of up to 174 individuals with 11 Federal agencies. In the other investigation, CBP OPR shared the sensitive PII of up to 4,825 individuals multiple times with 30 agencies, although it was not clear these individuals had received in-person polygraph training. CBP OPR's own analysis of the individuals in the second investigation revealed that some may not have been Federal employees or applicants, located in the United States, or alive.

In both investigations, CBP OPR's collection, enhancement, and storage of the sensitive PII complied with the Privacy Act of 1974 and Department of Homeland Security policies. However, although CBP OPR was allowed to share the sensitive PII with other Federal agencies, we do not believe the sharing of information with 30 agencies in the second investigation met the intent of what was allowed. Further, the manner in which the information was shared violated aspects of the Privacy Act of 1974 and DHS policies. Specifically, CBP OPR staff did not appropriately document disclosure of the sensitive PII, password protect it, or properly restrict its further dissemination. Because of this lack of protection, each time the sensitive PII was shared its vulnerability increased. We believe the manner in which CBP OPR shared the sensitive PII showed a lack of regard for, and may have compromised these individuals' privacy. We attribute this to CBP OPR's general belief that accomplishing its law enforcement mission takes precedence over its responsibility to protect individuals' privacy.

ICE Still Struggles to Hire and Retain Staff for Mental Health Cases in Immigration Detention

Number: OIG-16-113-VR
Date: 07/21/2016
Summary: In our 2011 report, we made three recommendations aimed at addressing challenges in attracting and retaining mental health care providers, such as psychiatrists. Although we closed these recommendations and ICE has taken steps to implement them, IHSC continues to struggle attracting and retaining mental health care providers. For instance, ICE officials explained it is difficult to attract and retain psychiatrists at detention facilities in rural and remote areas. With high demand in the public and private sectors for mental health care providers, IHSC has to compete to hire providers. As we reported in 2011, IHSC still cannot offer competitive salaries, especially for psychiatrists. In addition, ICE's lengthy security clearance process continues to discourage candidates from waiting for an ICE offer once they receive other offers.

IHSC has attempted to mitigate staffing difficulties by using Title 38 of the U.S. Code,1 which helps Federal agencies to better compete with nonfederal employers through more flexible recruitment, retention, and pay than that of the civil service. For example, ICE officials said they used Title 38 hiring authorities to recruit and pay for critically needed health care personnel, such as psychiatrists and registered nurses. According to ICE officials, although they have made progress, staffing challenges are likely to continue because the contributing factors are mainly outside of their control. We requested, but did not receive, documentation to support this assertion and to quantify the staffing issues. ICE needs to maintain data and provide evidence to substantiate the ongoing challenges outside of its control and the continuing staffing limitations.

At the beginning of our verification review, five recommendations from the March 2011 report remained open. We sought to determine the status of the recommendations and whether ICE fully implemented corrective actions. ICE gradually gave us updated action plans and documentation to support closing these recommendations. Specifically, ICE provided policies and guidance for:

- requesting mental health information from non-ICE facilities upon taking custody of a detainee;
- identifying detainees with mental health conditions to immigration courts and facilitating their access to legal representation; and
- using tele-psychiatry at detention facilities used by ICE.

After reviewing ICE's explanations and documentation, we consider these recommendations resolved and closed.

We plan to continue the Office of Inspector General's (OIG) oversight in this area to ensure that ICE provides appropriate care to detainees with mental health conditions. For example, we are initiating periodic inspections of facilities housing ICE detainees based on concerns raised by immigrant rights groups about conditions for detainees in ICE custody. If they arise, we will also review other serious detainee mental health-related issues.

Management Advisory -DHS Should Better Evaluate the Performance of Its Working Capital Fund

Number: OIG-16-108
Date: 07/01/2016
Summary: Through this management advisory, we are bringing to your attention improvements that could be made to the Department of Homeland Security Working Capital Fund (WCF). First, the Department does not have performance measures to help determine its progress in meeting the WCF's goals to centralize and improve the management of services, reduce costs, and develop budgeting and expenditure plans for services. Second, DHS does not conduct consistent and regular reviews of some services funded by the WCF. Consistent and regular reviews would help determine whether funding activities through the WCF is more cost effective than using non-WCF funding. Because of these deficiencies, DHS cannot be certain it is using the WCF as fully as possible to improve cost effectiveness and efficiency.

DHS' Use of Reimbursable Work Agreements with GSA

Number: OIG-16-105
Date: 06/23/2016
Summary: Department of Homeland Security components are not always in compliance with requirements when using reimbursable work agreements (RWA). We reviewed 20 RWAs and are questioning 10 RWAs with obligated funds of more than $47 million that did not comply with requirements. Components did not always provide evidence that statements of work were prepared and submitted to the General Services Administration (GSA) or that detailed cost estimates for the work to be performed were on file as required. Additionally, some components were not able to reconcile RWA expenditures with GSA's records or provide evidence that unused funds were deobligated at closeout. This occurred because of limited policies, poor controls, and inconsistent oversight in DHS' RWA process.

As a result, DHS cannot ensure work performed by GSA was in accordance with expectations and plans. Components cannot determine whether the costs to complete the work are reasonable or valid, which may lead to unnecessary costs and funds that could have been put to better use.

DHS Does Not Have Comprehensive Policies or Training for Off-duty Conduct of Employees Traveling and Working Abroad

Number: OIG-16-95
Date: 05/27/2016
Summary: Neither DHS nor the six DHS components with the largest international presence have comprehensive policies and training to govern employees' off-duty conduct while abroad. DHS has some limited, department-wide policies for off-duty conduct in general, but they do not specifically address employee conduct abroad; the six components' policies do not cover some aspects of conduct, such as drinking excessive amounts of alcohol and using drugs. DHS as a whole does not offer training in off-duty conduct for employees traveling and working abroad. One component offers training to those working abroad, but only one of the six offers training to both travelers and

those working abroad. As of August 2015, DHS had nearly 1,500 employees working in 80 countries, and DHS employees make thousands of trips abroad. To minimize the risk of misconduct and its potential negative effect on the Department's ability to accomplish its mission, DHS should ensure it has comprehensive policies specifically addressing off-duty conduct abroad and make certain all employees traveling and working abroad are adequately trained and acknowledge and understand these policies.

Department of Homeland Security's FY 2015 Compliance with the Improper Payments Elimination and Recovery Act of 2010

Number: OIG-16-88
Date: 05/11/2016
Summary: Although DHS met all the reporting requirements of IPERA, it did not meet its annual reduction targets established for each high-risk program as required by OMB. As such, we concluded that DHS did not fully comply with IPERA.

Additionally, we reviewed DHS' processes and procedures for estimating its annual improper payment rates. Based on our review, we determined DHS did not properly perform oversight of the components' improper payment testing and reporting. Specifically, DHS RM&A did not properly document its review of the components' risk assessments.

DHS Contracts and Grants Awarded through Other Than Full and Open Competition FY 2015

Number: OIG-16-58
Date: 04/05/2016
Summary: In FY 2015, DHS awarded 453 noncompetitive contracts worth about $229 million. This represents a downward trend of more than $3 billion obligated through noncompetitive contracts over an 8-year period. We reconciled the Department's FY 2015 contract listing against the Federal Procurement Data System and found that the data between the two lists were more than 99 percent identical.

Also in FY 2015, DHS awarded 63 noncompetitive grants worth about $127 million. Although one noncompetitive grant worth approximately $419,000 did not meet accuracy, timeliness, or completeness standards, more than 98 percent did meet the requirements as set forth in the Federal Funding Accountability and Transparency Act of 2006.

Department of Homeland Security's FY 2014 Compliance with the Improper Payments Elimination and Recovery Act of 2010 (Revised)

Number: OIG-15-94
Date: 02/22/2016
Summary: Although DHS met all the reporting requirements of IPERA, it did not meet its annual reduction targets established for each high-risk program as required by OMB. As such, we concluded that DHS did not fully comply with IPERA.

Our retesting also showed that FEMA properly performed IPERA payment testing for three programs.

However, DHS could improve its oversight and review of IPERA risk assessments. DHS' RM&A was delayed in approving the components' risk assessments and sample test plans, which it attributed to staffing shortages. The components began improper payment testing before obtaining RM&A's approval. In addition, neither FEMA nor RM&A noticed FEMA's omission of one program that should have been included in its risk assessments. As a result of our review, however, FEMA did perform a risk assessment of that program.

Department of Homeland Security's FY 2013 Compliance with the Improper Payments Elimination and Recovery Act of 2010 (Revised)

Number: OIG-14-64
Date: 02/19/2016
Summary: In fiscal year (FY) 2010, the Federal government's total improper payment amount reached $121 billion. In that same year, Congress passed the Improper Payments Elimination and Recovery Act of 2010 (IPERA or the Act) in an effort to reduce improper payments. In addition to reducing improper payments, the Act requires each agency's Inspector General to determine whether the agency complies with the Act annually. Since the implementation of the Act, DHS has reduced its improper payment amount from $222 million in FY 2011 to $178 million in FY 2013. Our audit objective was to determine whether the Department of Homeland Security (DHS) complied with the Act in fiscal year 2013. In addition, we also evaluated the accuracy and completeness of DHS' improper payment reporting and its efforts to reduce and recover improper payments for fiscal year 2013.

Although DHS met all the reporting requirements of the Act, it did not meet its annual reduction targets established for each program deemed susceptible to improper payments. As such, we concluded that DHS did not fully comply with IPERA.

We reviewed the accuracy and completeness of DHS' improper payment reporting and DHS' efforts to reduce and recover improper payments. DHS has made significant improvements to its processes in the past year to help ensure the accuracy and completeness in reporting improper payments and in its efforts to reduce and recover overpayments. Specifically, in the past year DHS has—

- segregated duties appropriately;
- improved its review processes to help ensure that components' risk assessments are properly supported;
- improved its policies and procedures to identify, reduce, and report improper payments; and
- improved its improper payment recovery efforts.

In January 2016, we made one new recommendation in this report.

Department of Homeland Security's FY 2012 Compliance with the Improper Payments Elimination and Recovery Act of 2010 (Revised)

Number: OIG-13-47
Date: 02/19/2016
Summary: In fiscal year 2010, the Federal Government's total improper payment amount was at a high of $121 billion. In that same year, Congress passed the Improper Payments Elimination and Recovery Act of 2010 (IPERA or the Act) in an effort to reduce improper payments. Since fiscal year 2010, the Federal Government's total improper payment rate has declined to $115 and $108 billion for fiscal years 2011 and 2012, respectively. In addition to reducing improper payments, the Act requires each agency's Inspector General to annually determine if the agency is in compliance with the Act.

Our audit objective was to determine whether the Department of Homeland Security (DHS) complied with the Act. In addition, we also evaluated the accuracy and completeness of DHS' improper payment reporting and its efforts to reduce and recover improper payments for fiscal year 2012.

Although DHS met all the reporting requirements of the Act, it did not meet its annual reduction targets established for each high-risk program as required by the Office of Management and Budget. As such, we concluded that DHS did not fully comply with IPERA.

We reviewed the accuracy and completeness of DHS' improper payment reporting and its efforts to reduce and recover improper payments. DHS needs to improve internal controls to ensure the accuracy and completeness of improper payment reporting. Specifically, it needs to improve its review processes to ensure that the risk assessments properly support the components' determination of programs susceptible to significant improper payments. Furthermore, DHS needs to adequately segregate duties and improve its policies and procedures to identify, reduce, and report improper payments.

We made nine recommendations that if implemented would improve the accuracy and completeness of DHS' improper payment reporting and improve its efforts to recover any overpayments. The Department concurred with all of the recommendations.

DHS Needs to Improve Implementation of OCFO Policy Over Reimbursable Work Agreements

Number: OIG-16-39
Date: 02/18/2016
Summary: Components are not issuing RWAs in compliance with the Department's policy. Specifically, 100 percent of the 43 RWAs we tested—totaling approximately $88 million—had not been reviewed by a Certified Acquisition Official (CAO). In January 2015, DHS issued a policy requiring components to have a CAO review RWAs to ensure they are being issued properly prior to obligating funds. The CAO plays a critical role in ensuring high-risk transactions receive proper oversight. However, 70 percent of the RWAs we tested did not include enough information for a CAO to make an informed decision. DHS did not ensure components updated their policies and

procedures to reflect the new requirements. Without a CAO review, components may continue to improperly issue RWAs, circumventing acquisition controls.

DHS' Oversight of Its Workforce Training Needs Improvement

Number: OIG-16-19
Date: 01/20/2016
Summary: DHS does not have adequate oversight of its workforce training. DHS lacks reliable training cost information and data needed to make effective and efficient management decisions. In addition, it does not have an effective governance structure for its training oversight, including clearly defined roles, responsibilities, and delegated authorities. Finally, DHS has not adequately addressed 29 different recommendations to improve training efficiencies made since 2004 by various working groups. As a result, DHS cannot ensure the most efficient use of resources.

FEMA Faces Challenges in Managing Information Technology

Number: OIG-16-10
Date: 11/20/2015
Summary: The Federal Emergency Management Agency (FEMA) has taken steps to improve its IT management since our 2011 audit, but more remains to be done. Specifically, FEMA has developed numerous IT planning documents but has not effectively coordinated, executed, or followed through on these plans. Without effective IT planning, FEMA risks making limited progress improving IT needed to support the agency's mission. Although FEMA has improved its IT governance through establishing an IT Governance Board, these efforts have not yet been fully effective.

FEMA has struggled to implement effective agency-wide IT governance, in part because the Chief Information Officer has not had sufficient control and budget authority to effectively lead the agency's decentralized IT environment. Without effective agency-wide IT governance, FEMA's IT environment has evolved over time to become overly complex, difficult to secure, and costly to maintain.

Further, in this complex, decentralized IT environment, FEMA's IT systems are not sufficiently integrated and do not provide personnel with the data search and reporting tools they need. As a result of system limitations, end users engage in inefficient, time-consuming business practices that can increase the risk that disaster assistance and grants could be delayed and duplication of benefits could occur.

Security Concerns with Federal Emergency Management Agency's eGrants Grant Management System

Number: OIG-16-11
Date: 11/19/2015
Summary: Since 2001, FEMA provided first responder organizations with more than $9 billion through the AFG and Staffing for Adequate Fire and Emergency Response (SAFER) programs.

According to FEMA, it began using the eGrants system in 2003 to manage the funds awarded through these programs. However, the eGrants system does not comply with Department of Homeland Security (DHS) information system security requirements. Specifically, access to the eGrants system is not controlled or limited because FEMA instructs grantees to share usernames and passwords within the grantee's organization and with contractors who manage grants. As a result, someone other than the primary point of contact can take action or make changes in eGrants without the grantee's knowledge.

Additionally, in June 2014, DHS's Office of Cyber Security advised FEMA it should not authorize eGrants to operate because it poses an unacceptable level of risk to the agency. FEMA's Chief Information Officer acknowledged the high level of risk posed by system deficiencies and vulnerabilities. Despite the known system deficiencies and risks,

Major Management and Performance Challenges Facing the Department of Homeland Security

Number: OIG-16-07
Date: 11/13/2015
Summary: DHS' mission to protect the Nation entails a wide array of responsibilities. These range from facilitating the flow of commerce and travelers, countering terrorism, and securing and managing the border to enforcing and administering immigration laws and preparing for and responding to natural disasters.

This report identifies major challenges that affect the Department as a whole, as well as its individual components, who work together to achieve this multi-faceted mission. The following list represents the nine areas of most persistent concern for the Department:
DHS Management and Operations Integration

- Acquisition Management
- Financial Management
- Information Management and Technology
- Transportation Security
- Border Security and Immigration Enforcement
- Disaster Preparedness and Response
- Infrastructure Protection and Cybersecurity
- Employee Accountability and Integrity

Within each of the nine areas are specific challenges the Department faces in supporting an engaged, connected workforce; identifying and monitoring business processes that are understandable and streamlined; and designing and implementing innovative technologies that address mission needs. Without the right processes and technology, the Department's strongest asset — its people — may be hampered in their ability to accomplish the Department's mission most effectively and efficiently.

Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting

Number: OIG-16-06
Date: 11/13/2015
Summary: The independent public accounting firm KPMG LLP has issued an unmodified (clean) opinion on DHS' consolidated financial statements. In the independent auditors' opinion, the financial statements present fairly, in all material respects, DHS' financial position as of September 30, 2015.

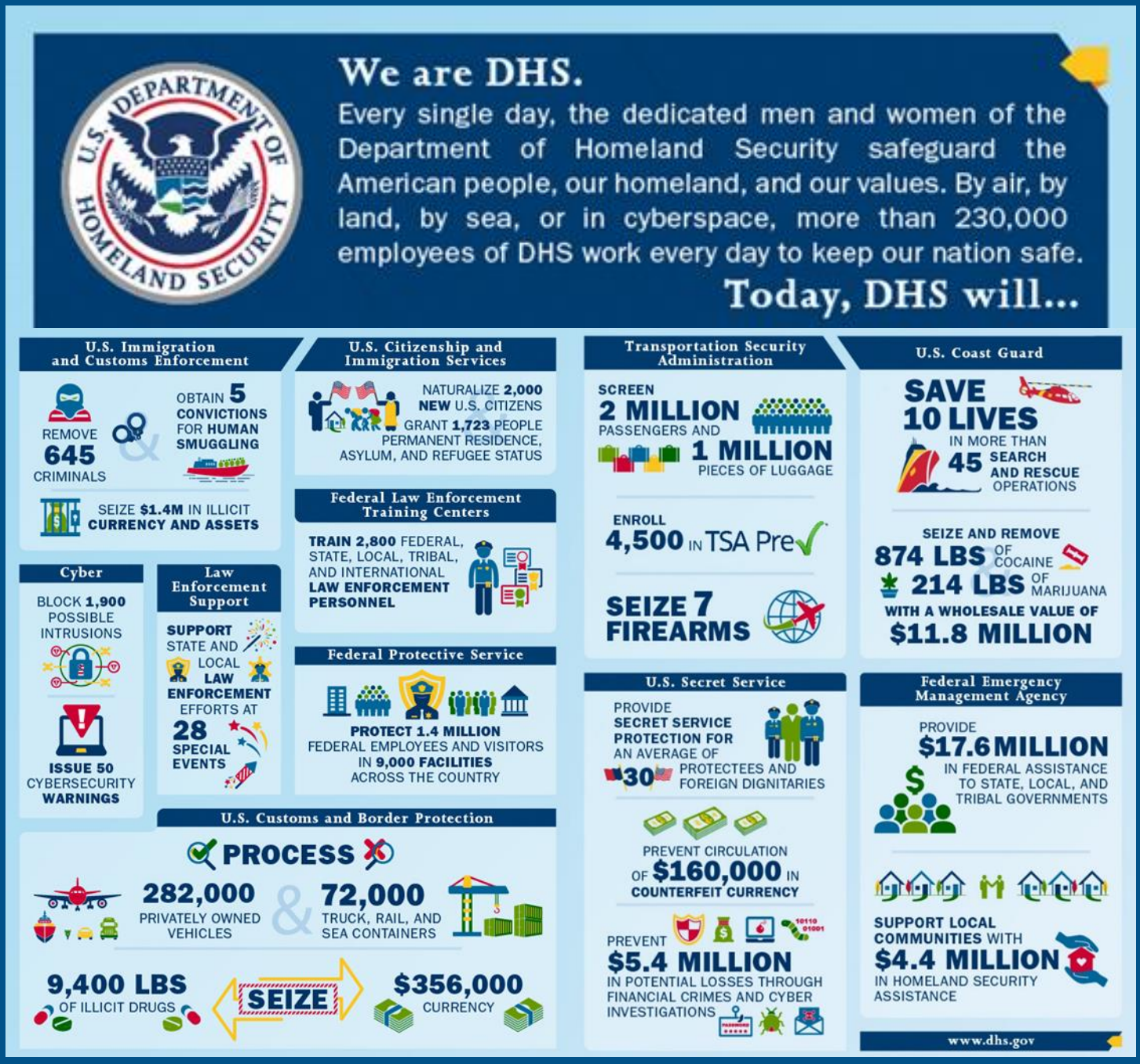
KPMG LLP issued an adverse opinion on DHS' internal control over financial reporting of its financial statements as of September 30, 2015. The report identifies seven significant deficiencies in internal control; three of which are considered material weaknesses. The material weaknesses are in financial reporting; information technology controls and financial system functionality; and property, plant, and equipment. The report also identifies instances of noncompliance with four laws and regulations.

Component Acronyms

Below is the list of DHS Components and their Acronyms.

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

Homeland
Security



As of September 14, 2016 (unaudited)

Homeland Security