Annual Performance Report

Fiscal Years 2017-2019

Appendix B: Relevant GAO and OIG Reports

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) 2017-2019 presents the Department's performance measures and applicable results, provides the planned performance targets for FY 2018 and FY 2019, and includes information on the Department's Strategic Review and our Agency Priority Goals. Additionally, this report presents information on the Department's reform agenda (in compliance with Executive Order 13781), regulatory reform, the Human Capital Operating Plan, and a summary of our performance challenges and high-risk areas identified by the DHS Office of the Inspector General and the Government Accountability Office. The report is consolidated to incorporate our annual performance plan and annual performance report.

For FY 2017-2019, the Department is using the alternative approach—as identified in the Office of Management and Budget's Circular A-136—to produce its Performance and Accountability Reports, which consists of the following three reports:

- DHS Agency Financial Report | Publication date: November 15, 2017.
- DHS Annual Performance Report | Publication date: February 5, 2018
- DHS Report to our Citizens (Summary of Performance and Financial Information) | Publication date: February 2018.

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

Contact Information

For more information, contact:

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

Information may also be requested by sending an email to par@hq.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 2017 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, extracted 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 2017 DHS OIG reports is available at:
https://www.oig.dhs.gov/reports/audits-inspections-and-evaluations

Analysis and Operations (AO)

GAO Reports

Countering ISIS and Its Effects: Key Issues for Oversight

Number: GAO-17-687sp
Date: 7/18/2017
Summary: In September 2014, the White House issued the U.S. Strategy to Counter the Islamic State of Iraq and the Levant (ISIL) with the goal to degrade and destroy ISIS through an approach that included working with regional and international partners. The Department of Defense (DOD) reported that it has allocated $10.9 billion for counter-ISIS operations from August 2014—when these operations began—through 2016. The Department of State (State) and the U.S. Agency for International Development (USAID) report having allocated more than $2.4 billion in funding for Iraq, Jordan, Lebanon, and Syria to counter ISIS, respond to and mitigate the Syrian crisis, bolster regional security, and support development programs. State and USAID also report that, separate from U.S. political efforts to counter ISIS, the two agencies have provided more than $1.3 billion in humanitarian assistance to Iraqis in the region since fiscal year 2014 and more than $6.5 billion in humanitarian assistance to Syrians and others in the region affected by the Syrian crisis. Given the importance of this issue as a U.S. national security priority and the level of resources expended to counter ISIS and address humanitarian and other effects related to these efforts, GAO identified a number of key issues for the 115th Congress to consider in developing oversight agendas and determining the way forward. Significant oversight will be needed to help ensure visibility over the cost and progress of these efforts. DHS plays a vital role in this effort and is discussed in several areas throughout the report.

DHS OIG Reports

(U) Annual Evaluation of DHS' INFOSEC Program (Intel Systems - DHS Intelligence and Analysis) for FY 2016

Number: OIG-17-58-UNSUM
Date: 5/9/2017
Summary: The OIG reviewed DHS's information security program for intelligence systems in accordance with requirement of the Federal Information Security Modernization Act. The objective of the review was to determine whether DHS's information security program and practices are adequate and effective in protecting the information and information systems supporting DHS's intelligence operations and assets. The OIG assessed DHS programs for continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, plans of action and milestones, remote access management, contingency planning, and contractor systems.

Review of Domestic Sharing of Counterterrorism Information

Number: OIG-17-49
Date: 3/30/2017
Summary: Fifteen years after the September 11, 2001, terrorist attacks on the United States, the terrorist threat remains in the United States and abroad, as evidenced by recent attacks in Paris, France; San Bernardino, California; Brussels, Belgium; Orlando, Florida; and Nice, France. The U.S.'s national security depends on the ability to share the right information with the right people at the right time. This requires sustained and responsible collaboration among federal, state, local, and tribal entities, as well as the private sector and international partners.

In response to a request from the Senate Select Committee on Intelligence, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Judiciary Committee, the Offices of Inspector General (OIG) of the Intelligence Community (IC), DHS, and the Department of Justice (DOJ) conducted a review of the domestic sharing of counterterrorism information.

The OIGs concluded that the partners in the terrorism-related Information Sharing Environment – components of the Office of the Director of National Intelligence (ODNI), DHS, DOJ, and their state and local partners – are committed to sharing counterterrorism information. The partners' commitment to protecting the nation is illustrated by the actions taken before, during, and following terrorism-related incidents, as well as by programs and initiatives designed to improve sharing of counterterrorism information. However, the OIGs also identified several areas in which improvements could enhance information sharing.

Countering Weapons of Mass Destruction (CWMD) Office

GAO Reports

Radiation Portal Monitors: DHS's Fleet Is Lasting Longer than Expected, and Future Acquisitions Focus on Operational Efficiencies

Number: GAO-17-57
Date: 10/31/2016
Summary: The Department of Homeland Security's (DHS) assessment of its fleet of radiation portal monitors (RPM)—large, stationary radiation detectors through which vehicles and cargo containers pass at ports of entry—shifted over time and, as a result, DHS has changed the focus of its RPM replacement strategy. During fiscal years 2014 and 2015, as some RPMs began to reach the end of their estimated 13-year service life, DHS began planning for replacing the entire fleet of almost 1,400 RPMs. However, as of September 2016, the fleet remains nearly 100 percent operational and recent studies indicate that the fleet can remain operational until at least 2030 so long as proactive maintenance is carried out and RPM spare parts remain available. As a result, in 2016, DHS changed the focus of its RPM replacement strategy to selective replacement of RPMs—using existing RPMs that have been upgraded with new alarm threshold settings or purchasing enhanced, commercially available RPMs—to gain operational efficiencies and reduce labor requirements at some ports.

During fiscal years 2016 through 2018, DHS plans to replace approximately 120 RPMs along the northern U.S. border with upgraded RPMs and, during fiscal years 2018 through 2020, plans to replace between 150 and 250 RPMs at select high-volume ports with enhanced, commercially available RPMs. Specifically, DHS plans to replace some legacy RPMs—those that cannot be upgraded with the new alarm thresholds—at northern U.S. land border crossings with RPMs from existing inventory that have been upgraded. This upgrade enables improved threat discrimination and minimizes "nuisance" alarms created by naturally occurring radioactive materials (NORM) in commonly shipped cargo such as ceramics, fertilizers, and granite tile. Improved discrimination between NORM and threat material will create efficiencies for the movement of cargo through ports and minimize time that DHS's Customs and Border Protection (CBP) officers spend adjudicating the nuisance alarms. DHS is also planning limited replacement of upgraded RPMs at select high-volume ports with enhanced, commercially available RPMs that offer nuisance alarm levels significantly lower than even the upgraded RPMs. Currently, upgraded RPMs at some high-volume ports do not reduce nuisance alarm rates enough to implement remote RPM operations—which allows CBP officers to carry out other duties at the ports when not responding to an RPM alarm—because of the high number of vehicles and cargo containers passing through the ports daily.

DHS OIG Reports

No DHS OIG reports were available that aligned to this Component.

Customs and Border Protection (CBP)

GAO Reports

U.S. Customs and Border Protection: Contracting for Transportation and Guard Services for Detainees

Number: GAO-17-89R
Date: 9/27/2016
Summary: CBP is responsible for apprehending aliens illegally entering the United States. CBP coordinates the movement, security, and monitoring of its detained or inadmissible individuals, who can be moved to or from several locations with and across Border Patrol sectors while in CBP's custody. CBP uses a private contractor to assist Border Patrol with transportation and guard services for aliens apprehended at or between ports on the southwest boarder. This report examines to what extent CBP manages its existing transportation services contract to meet its needs and assesses the performance of the contractor responsible for transporting detained individuals.

CBP's current transportation service contract, expected to expire on or around March 3, 2019, include securing detainee land transportation from point of apprehension, station to station, station to port of entry for removal; detainee escort services; court security transportation; medical escort and guard services of detainees in DHS Custody while at a medical treatment facility; and other detainee monitoring duties to meet CBP's operational requirements throughout the southwest

boarder. The required services supporting CBP are performed in seven of the nine southwest boarder sectors of San Diego, Yuma, Tucson, El Paso, Del Rio, Laredo, Rio Grande Valley and CBP field offices, ports, highway checkpoints, processing centers, hospital, courts and detention centers. In FY 2016 the contractor has transported between 75 and 79% of detainees in the southwest sectors and Border Patrol has transported the remainder.

GOA found that CBP assigns roles and responsibilities to manage contract performance both at the CBP headquarters and sector levels and has the flexibility to reallocate contractor resources where necessary through day-to day coordinate, oversight and management of the contract. GAO found that CBP included mechanisms in the contract to allow for day-to-day changes to transportation routes and vehicles used in order to achieve sector transportation service needs. In addition, sectors also have the flexibility to reallocate labor and vehicle hours to meet the variations in medical escort, facilities guard, and transport service needs at different points of time. In addition, CBP implemented a quality assurance plan, that is aligned with Federal Acquisition Regulation standards and OMB guidance, which directs contract oversight at both the headquarters and sector levels. As a result CBP is able to conduct a variety of contract oversight activities to ensure that measure outlined by the contract are met, assess performance, and perform quality assurance. In addition, GAO found that CBP is able to conduct quarterly program management reviews on contract performance which has been used as a tool to identify future requirements and lessons learned and provide opportunities for information sharing.

Border Security: CBP Aims to Prevent High-Risk Travelers from Boarding U.S.-Bound Flights, but Needs to Evaluate Program Performance

Number: GAO-17-216
Date: 1/24/2017
Summary: CBP, through National Targeting Center (NTC), is responsible for analyzing traveler data and threat information to identify high-risk travelers before they board U.S.-bound flights. NTC conducts traveler data matching which assesses whether travelers are high-risk by matching their information against U.S. government databases and lists, and rules-based targeting, which enables CBP to identify unknown high-risk individuals at Preclearance locations. CBP uses the results of NTC's analyses to help identify and interdict high-risk travelers before they board U.S.-bound flights. CBP officers inspect all U.S. bound travelers on precleared flights at the 15 Preclearance locations in six countries and, if deemed inadmissible, a traveler will not be permitted to board the aircraft. CBP also operates nine Immigration Advisory Program (IAP) and two Joint Security Program (JSP) locations as well as three Regional Carrier Liaison Groups (RCLG) that allow CBP to work with foreign government and air carrier officials to identify and interdict high-risk travelers. According to CBP, in FY 2015 there were over 22,000 high-risk air travelers that were identified and interdicted through its pre-departure programs and 10,648 of the approximately 16 million air travelers seeking admission through Preclearance locations that were inadmissible. Additionally, CBP made 11,589 no-board recommendations to air carriers for the approximately 88 million air travelers bound for the United States.

This report addresses (1) how CBP identifies high-risk travelers before they board U.S.-bound flights; (2) the results of CBP's pre-departure programs and the extent to which CBP has measures to assess program performance; and (3) how CBP plans to expand its pre-departure programs.

According to GAO, although CBP has taken some initial steps to measure the performance of its air pre-departure programs, it has not fully evaluated the effectiveness of its pre-departure programs as a whole, including implementing a system of performance measures and baselines to assess whether the programs are achieving their stated goals. GAO found that CBP primarily focuses on the high level objectives such as enhancing national security, counterterrorism, and travel facilitation and does not assess the performance of the program operations on a regular basis, in part because it has not established baselines for these measures. As a result, CBP doesn't have anything against which to compare the data to determine whether the programs are achieving stated goals. GAO found that solely tracking increases or decreases in program data, such as traveler volume or the number of invalid travel documents seized, does not allow CBP to fully evaluate its pre-departure programs as such changes in the data may not be an indicator of program success or increased efficacy. GAO recommended that CBP develop and implement a system of performance measures and baselines to evaluate the effectiveness of its pre-departure programs and assess whether the programs are achieving their stated goals

GAO found that although Preclearance expansion is a significant priority for CBP, there has been challenges in CBP's ability to expand to all priority locations. According to CBP, opening a new Preclearance location depends on the willingness and readiness of the host foreign government and requires an international agreement and resolution of various diplomatic issues such as the extent of the law enforcement capability of CBP officers within the host country to include the carriage of service weapons, CBP officer immunity or legal status within the host country, and other complex issues. Other challenges included staffing gap which CBP is working to resolve through hiring efforts and staffing modeling to determine staffing needs. According to CBP officials, the total staff required for each new pre-departure location depends on the negotiated CBP presence at each location.

Supply Chain Security: Providing Guidance and Resolving Data Problems Could Improve Management of the Customs-Trade Partnership Against Terrorism Program

Number: GAO-17-84
Date: 2/8/2017
Summary: CBP is responsible for administering cargo security and facilitating the flow of legitimate commerce. CBP has implemented several programs such as Customs-Trade Partnership Against Terrorism (C-TPAT), as part of a layered strategy for overseeing global supply chain security. C-TPAT aims to secure the flow of goods bound for the United States through voluntary antiterrorism partnerships with entities that are stakeholders within the international trade community. As a first step in C-TPAT membership, an entity must sign an agreement with CBP signifying its commitment to enhance its supply chain security practices consistent with C-TPAT minimum security criteria and to work to enhance security throughout its global supply chain to the United States. The partnership agreements that C-TPAT members sign provide CBP with the authority it needs to validate members' security practices. In return, members are eligible to receive benefits, such as a reduced likelihood their shipments will be examined. GOA reported, as of September 2016, there were 11,490 C-TPAT members of which 37 percent were importers and the remaining 63 percent of C-TPAT members were distributed among other trade industry sectors. In 2008, CBP expanded C-TPAT membership to include other trade industry sectors, such as third party logistics providers and exporters.

This report assesses the extent to which (1) CBP is meeting its security validation responsibilities, and (2) C-TPAT members are receiving benefits. GAO reviewed information on security validations, member benefits, and other program documents and reported that C-TPAT program has faced challenges in meeting C-TPAT security validation responsibilities because of problems with the functionality of the program's data management system. In 2015, C-TPAT staff identified instances in which the system incorrectly altered C-TPAT members' certification or security profile dates, requiring manual verification of member data and impairing the ability of C-TPAT security specialists to identify and complete required security validations in a timely and efficient manner. In addition, GAO found that security specialists had difficulty with reviewing and completing security validation because they were not able to access and save data.

Border Security: Additional Actions Needed to Strengthen Collection of Unmanned Aerial Systems and Aerostats Data

Number: GAO-17-152
Date: 2/16/2017
Summary: U.S. Customs and Border Protection (CBP) uses Predator B unmanned aerial systems (UAS) for a variety of border security efforts, such as missions to support investigations in collaboration with other government agencies and to locate individuals illegally crossing the border. This report addresses the following questions: (1) How does CBP use the Predator B unmanned aerial systems (UAS) and aerostats for border security activities, and to what extent has CBP developed and documented procedures for UAS coordination and (2) To what extent has CBP taken actions to assess the effectiveness of its UAS and aerostats for border security activities?

GAO reported that as of fiscal year 2016, CBP operates nine Predator B aircraft from four Air and Marine Operations (AMO) National Air Security Operations Centers (NASOC) in Arizona, Florida, Texas, and North Dakota. Based on CBP data provided to GAO for fiscal year 2015, annual obligations for CBP's Predator B program were approximately $42 million and the cost per flight hour was $5,878.18. AMO is responsible for operation of CBP's Predator B aircraft and coordinates with other CBP components and government agencies to perform federal border security activities.

CBP uses aerostats—unmanned buoyant craft tethered to the ground and equipped with video surveillance cameras and radar technology—to support its border security activities along the southern U.S. border. In south Texas, the U.S. Border Patrol uses relocatable tactical aerostats equipped with video surveillance technology to locate and support the interdiction of cross-border illegal activity. At eight fixed sites across the southern U.S. border and in Puerto Rico, CBP uses the Tethered Aerostat Radar System (TARS) program to support its efforts to detect occurrences of illegal aircraft and maritime vessel border incursions.

GAO found that CBP established various mechanisms to coordinate with other agencies for Predator B missions but did not develop and document coordination procedures in two of its three operational centers. Without documented coordination procedures in all operating locations consistent with internal control standards, CBP does not have reasonable assurance that practices in all operating locations align with existing policies and procedures for joint operations with other federal and non-federal government agencies.

GAO also found that CBP has taken actions to assess the effectiveness of its UAS and aerostats for border security, but could improve its data collection. CBP collects a variety of data on its use of Predator B UAS, tactical aerostats, and TARS including data on their support for the apprehension of individuals, seizure of drugs, and other events (asset assists). For Predator B UAS, GAO found mission data—such as the names of supported agencies and asset assists for seizures of narcotics—was not recorded consistently across all operational centers, limiting CBP's ability to assess the effectiveness of the program.

GAO made five recommendations, including that CBP document coordination procedures for UAS operations in all operating locations and update guidance and implement training for collection of Predator B mission data.

Southwest Border Security: Additional Actions Needed to Better Assess Fencing's Contributions to Operations and Provide Guidance for Identifying Capability Gaps

Number: GAO-17-331
Date: 2/19/2017
Summary: In an effort to secure the United States border between ports of entry, CBP invested a total of $2.4 billion between fiscal years 2007 and 2015 to deploy tactical infrastructure (TI) — fencing, gates, roads, bridges, lighting, and drainage infrastructure—along the nearly 2,000 mile southwest border. This report reviews the use of border fencing along the southwest border and examines (1) border fencing's intended contributions to border security operations and the extent to which CBP has assessed these contributions and (2) the extent that CBP has processes in place to ensure sustainment and deployment of TI along the southwest border and challenges in doing so.

Border Patrol officials reported to GAO that TI facilitates the capabilities for impedance and denial and operational mobility and that border fencing, including pedestrian and vehicle fencing, is intended to facilitate the impedance and denial by diverting and delaying illegal entries and roads and bridges are intended to facilitate the operational mobility by enabling agents to efficiently traverse their areas of responsibility.

GAO's found that, although CBP collects data it has not developed metrics that systematically use the data collected to assess the contributions of border fencing to its mission. Specifically, GAO found that CBP wasn't measuring the contributions of pedestrian and vehicular fencing to border security operations as part of a system of capabilities along the southwest border and lacked documented guidance on requirement management process for identifying TI and other operational requirements for border security operations.

Border Security: DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain

Number: GAO-17-170
Date: 2/27/2017
Summary: This report highlights the DHS's efforts and limitations in developing and implementing a biometric exit capability to collect biometric data, such as fingerprints, from individuals exiting the United States. Since GAO's 2013 report CBP has conducted four pilot

programs to inform the development and implementation of a biometric exit system. This report examines the four pilot programs that CBP conducted and the various longstanding challenges with planning, infrastructure, and staffing that continue to affect CBP's efforts to develop and implement a biometric exit system.

GOA found, CBP has made progress in testing biometric exit capabilities, but various longstanding planning, infrastructure, and staffing challenges continue to affect CBP's efforts to develop and implement a biometric exit system. CBP is planning initial implementation of a biometric exit capability in at least one airport in 2018 and is working with airlines and airports on strategies for using public/private partnerships to reduce costs and give industry more control over how a biometric exit capability is implemented at airport gates. Despite, efforts, GAO found that CBP cannot complete the planning process until these partnership agreements and implementation decisions are finalized. Additionally, CBP continues to have infrastructure limitations that are challenging the implementation a biometric air exit capability. GAO noted that, according to CBP, U.S. airports generally do not have outbound designated secure areas for exiting travelers where biometric information could be captured by U.S. immigration officers. GAO determined that it is too early to assess the CBP's plans for developing and implementing a biometric exit capability and the extent to which those plans will address identified challenges, as CBP is in the process of finalizing its approach.

International Air Travelers: CBP Collaborates with Stakeholders to Facilitate the Arrivals Process, but Could Strengthen Reporting of Airport Wait Times

Number: GAO-17-470
Date: 3/30/2017
Summary: Within DHS, CBP, and airport and airline stakeholders jointly implement travel and tourism initiatives at U.S. international airports to facilitate the arrival of travelers. These initiatives include Automated Passport Control self-service kiosks that allow eligible travelers to complete a portion of the CBP inspection process before seeing a CBP officer, and Mobile Passport Control that allows eligible travelers to submit their passport and other information to CBP via an application on a mobile device. Various airport-specific factors can affect whether and how CBP and stakeholders implement travel and tourism facilitation initiatives at each airport. These factors include the size and layout of the airport facility, the infrastructure needed to support initiatives, the willingness and ability of the airport stakeholders to pay for initiatives or infrastructure to support them, as applicable, and stakeholder discretion in how to implement initiatives. CBP has two airport travel facilitation goals: (1) improving customer service levels for international arrivals and (2) maintaining or reducing wait times—and has implemented mechanisms to assess and obtain feedback on the traveler experience. This report examines (1) how CBP and stakeholders have implemented airport travel and tourism facilitation initiatives; (2) how CBP and stakeholders manage staff to facilitate the traveler entry process; and (3) the extent to which CBP has mechanisms to monitor and report wait times at U.S. international airports.

According to GAO, stakeholders provide resources to help facilitate the traveler entry process, and CBP allocates and manages staff using various tools. For example, CBP uses its Workload Staffing Model to determine the staffing requirements and help make allocation decisions for CBP officers at ports of entry, including airports. CBP also uses its Enterprise Management Information System to monitor and make immediate staffing changes to meet any traveler volume and wait time

concerns at airports. Airport and airline stakeholders can also enter into agreements to pay for CBP officers to work overtime during peak travel hours or outside regular operational hours.

CBP monitors airport wait times and reports data on its public website to help travelers plan flights, including scheduling connecting flights, but the reported data have limited usefulness to travelers. Currently, CBP does not report wait times by traveler type, such as U.S. citizen or foreign visitor. Rather, CBP reports average hourly wait times for all travelers on arriving international flights. By reporting wait times for all categories of travelers combined, CBP is reporting wait times that are lower than those generally experienced by visitors. According to GAO's analysis of CBP wait time data for the 17 busiest airports from May 2013 through August 2016, the average wait time was 13 minutes for U.S. citizens and 28 minutes for visitors, while the combined reported average wait time was 21 minutes. Reporting wait times by traveler type could improve the usefulness of CBP's wait time data to travelers by providing them with more complete and accurate data on their wait times. This could help inform their flight plans and could provide additional transparency to allow CBP to work with stakeholders to determine what, if any, changes are needed, to improve the traveler experience, and better manage wait times.

Border Security: DHS Could Strengthen Efforts to Establish Collaborative Mechanisms and Assess Use of Resources

Number: GAO-17-495T
Date: 4/4/2017
Summary: DHS and CBP have implemented various mechanisms along the southern U.S. border to coordinate security operations, but could strengthen coordination of Predator B unmanned aerial system (UAS) operations to conduct border security efforts. In September 2013, GAO reported that DHS and CBP used collaborative mechanisms along the southwest border—including interagency Border Enforcement Security Task Forces and Regional Coordinating Mechanisms—to coordinate information sharing, target and prioritize resources, and leverage assets. GAO interviewed participants from the various mechanisms who provided perspective on successful collaboration, such as establishing positive working relationships, sharing resources, and sharing information. Participants also identified barriers, such as resource constraints, rotation of key personnel, and lack of leadership buy-in. GAO recommended that DHS take steps to improve its visibility over field collaborative mechanisms. DHS concurred and collected data related to the mechanisms' operations. Further, as GAO reported in June 2014, officials involved with mechanisms along the southwest border cited limited resource commitments by participating agencies and a lack of common objectives. Among other things, GAO recommended that DHS establish written interagency agreements with mechanism partners, and DHS concurred. Lastly, in February 2017, GAO reported that DHS and CBP had established mechanisms to coordinate Predator B UAS operations but could better document their coordination procedures. GAO made recommendations for DHS and CBP to improve coordination of UAS operations, and DHS concurred.

GAO recently reported that DHS and CBP could strengthen efforts to assess their use of resources and programs to secure the southwest border. For example, in February 2017, GAO reported that CBP does not record mission data consistently across all operational centers for its Predator B UAS, limiting CBP's ability to assess program effectiveness. In addition, CBP has not updated its guidance for collecting and recording mission information in its data collection system since 2014. Updating guidance consistent with internal control standards would help CBP better ensure the

quality of data it uses to assess effectiveness. In January 2017, GAO found that methodological weaknesses limit the usefulness for assessing the effectiveness of CBP's Border Patrol Consequence Delivery System. Specifically, Border Patrol's methodology for calculating recidivism—the percent of aliens apprehended multiple times along the southwest border within a fiscal year—does not account for an alien's apprehension history over multiple years. Border Patrol could strengthen the methodology for calculating recidivism by using an alien's apprehension history beyond one fiscal year. Finally, CBP has not developed metrics that systematically use the data it collects to assess the contributions of its pedestrian and vehicle border fencing to its mission. Developing metrics to assess the contributions of fencing to border security operations could better position CBP to make resource allocation decisions with the best information available to inform competing mission priorities and investments. GAO made recommendations to DHS and CBP to update guidance, strengthen its recidivism calculation methodology, and develop metrics, and DHS generally concurred.

Federally Owned Vehicles: Agencies Should Improve Processes to Identify Underutilized Vehicles

Number: GAO-17-426
Date: 4/25/2017
Summary: Federal agencies spent more than $1.6 billion to purchase approximately 64,500 passenger vehicles and light trucks through the General Services Administration (GSA) from fiscal years 2011 through 2015. Five departments—Defense (DOD), Homeland Security (DHS), Agriculture (USDA), Justice, and Interior—purchased 90 percent of these vehicles, and spent a comparable percentage of the associated funds. The vehicles cost an average of approximately $25,600 each.

GAO determined that the three agencies reviewed—Navy within DOD, CBP within DHS, and Natural Resources Conservation Service (NRCS) within USDA—varied in efforts to determine if vehicles were utilized in fiscal year 2015. Navy determined that all of the 3,652 vehicles GAO selected for review were utilized by applying DOD and Navy criteria such as for mileage and individually justifying vehicles. CBP did not determine if 1,862 (81 percent) of its 2,300 selected vehicles were utilized in fiscal year 2015 even though the vehicles did not meet DHS's minimum mileage criteria. CBP officials stated that, contrary to DHS policy, CBP did not have criteria to measure these vehicles' utilization because it was difficult to manually collect the data needed to establish appropriate criteria and assess if vehicles met those criteria. CBP is currently installing devices in many of its vehicles that will allow it to more easily collect such data, but lacks a specific plan for how to ensure these data will allow it to determine if vehicles are utilized. NRCS did not determine if 579 (9 percent) of its 6,223 selected vehicles were utilized in fiscal year 2015. USDA and NRCS fleet officials stated that the agency did not annually assess vehicle utilization, nor did it apply USDA criteria such as mileage or days used. USDA and NRCS officials said they were unaware of USDA's policy requiring these steps because the policy had not been widely discussed or shared within USDA since 2012. CBP and NRCS cumulatively incurred an estimated $13.5 million in depreciation and maintenance costs in fiscal year 2015 for vehicles with unknown utilization (see table). While these costs may not equal the cost savings agencies derive from eliminating underutilized vehicles, without corrective action, agencies are incurring expenses to retain vehicles without determining if they are utilized.

Border Security: Additional Actions Could Strengthen DHS Efforts to Address Subterranean, Aerial, and Maritime Smuggling

Number: GAO-17-474
Date: 5/1/2017
Summary: GAO's analysis of DHS data showed that there were 67 discovered cross-border tunnels, 534 detected ultralight aircraft incursions, and 309 detected drug smuggling incidents involving panga boats (a fishing vessel) and recreational vessels along U.S. mainland borders from fiscal years 2011 through 2016. The number of known smuggling events involving these methods generally declined over this period, but they remain threats.

DHS has established various coordination mechanisms and invested in technology to address select smuggling methods in the subterranean, aerial, and maritime domains. For example, DHS established interagency task forces to investigate cross-border tunnels. However, DHS has not established comprehensive standard operating procedures for addressing cross-border tunnels, and we found that relevant officials were not aware of all DHS systems or offices with tunnel information. By establishing procedures for addressing cross-border tunnels, DHS could provide strategic guidance and facilitate information sharing department-wide, consistent with standards for internal control. DHS has also invested or plans to invest in at least five technology projects to help detect and track ultralight aircraft. However, DHS has not assessed and documented how all of the alternative ultralight aircraft technical solutions it is considering will fully address operational requirements or the costs and benefits associated with these different solutions. This type of analysis could help better position DHS to use its resources effectively and ensure that operational needs are met, consistent with risk management best practices.

DHS has established high-level smuggling performance measures and collects data on smuggling by tunnels, ultralight aircraft, panga boats, and recreational vessels; however, DHS has not assessed its efforts specific to addressing these smuggling methods to, for example, compare the percent of detected panga boat and recreational smuggling events that are interdicted against targeted performance levels. By establishing measures and regularly monitoring performance against targets, managers could obtain valuable information on successful approaches and areas that could be improved to help ensure that technology investments and operational responses to address these smuggling methods are effective, consistent with standards for internal control. This is a public version of a For Official Use Only—Law Enforcement Sensitive report that GAO issued in February 2017. Information DHS deemed For Official Use Only—Law Enforcement Sensitive has been redacted.

Border Security: Progress and Challenges in DHS's Efforts to Address High-Risk Travelers and Strengthen Visa Security

Number: GAO-17-599T
Date: 5/3/2017
Summary: In January 2017, GAO reported that CBP operates pre-departure programs to help identify and interdict high-risk travelers before they board U.S.-bound flights. CBP officers inspect all U.S.-bound travelers on precleared flights at the 15 Preclearance locations and, if deemed inadmissible, a traveler will not be permitted to board the aircraft. CBP also operates nine

Immigration Advisory Program and two Joint Security Program locations, as well as three Regional Carrier Liaison Groups, through which CBP may recommend that air carriers not permit identified high-risk travelers to board U.S.-bound flights. CBP data showed that it identified and interdicted over 22,000 high-risk air travelers through these programs in fiscal year 2015 (the most recent data available at the time of GAO's report). However, CBP had not fully evaluated the overall effectiveness of these programs using performance measures and baselines. CBP tracked some data, such as the number of travelers deemed inadmissible, but had not set baselines to determine if pre-departure programs are achieving goals, consistent with best practices for performance measurement. GAO recommended that CBP develop and implement a system of performance measures and baselines to better position CBP to assess if the programs are achieving their goals. CBP concurred and has established a working group to develop such measures and baselines.

In March 2011, GAO reported on the Visa Security Program (VSP) through which DHS's U.S. Immigration and Customs Enforcement (ICE) deploys personnel to certain U.S. overseas posts to review visa applications. Among other things, GAO found that ICE did not collect comprehensive data on all VSP performance measures or track the time officials spent on visa security activities. DHS did not concur with GAO's recommendations to address these limitations, stating that ICE collected data on all the required performance measures and tracked VSP case investigation hours. However, GAO continues to believe DHS needs to address these limitations. GAO has ongoing work assessing U.S. agencies' efforts to strengthen the security of the visa process, including oversight of VSP, in which GAO plans to follow up on the findings and recommendations from its March 2011 report related to ICE's efforts to enhance VSP performance measurement.

In May 2016, GAO reported on DHS's oversight of the Visa Waiver Program (VWP), which allows nationals from 38 countries to travel visa-free to the United States for business or pleasure for 90 days or less. GAO reported, among other things, that all 38 countries 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 shared such information. In August 2015, DHS established a new requirement for VWP countries to implement the latter two agreements; however, DHS did not establish time frames for instituting the amended requirements. GAO recommended that DHS work with VWP countries to implement these agreements and DHS concurred. As of April 2017, DHS reported that officials are continuing to work with VWP countries on time frames for implementing program requirements.

Customs and Border Protection: Improved Planning Needed to Strengthen Trade Enforcement

Number: GAO-17-618
Date: 6/12/2017
Summary: Two offices within CBP enforce U.S. trade laws and protect revenue. The Office of Trade develops policies to guide CBP's trade enforcement efforts, while the Office of Field Operations conducts a range of trade processing and enforcement activities at U.S. ports. CBP's previously port-centric approach to trade enforcement has shifted to a national-level, industry-focused approach with the establishment of the Office of Field Operations' 10 Centers of Excellence and Expertise. These Centers represent a shift in trade operations, centralizing the processing of

certain imported goods on a national scale through a single Center rather than individual ports of entry.

CBP conducts trade enforcement across seven high-risk issue areas using a risk-based approach, but its plans generally lack performance targets that would enable it to assess the effectiveness of its enforcement activities. Violations in the high-risk issue areas can cause significant revenue loss, harm the U.S. economy, or threaten the health and safety of the American people. CBP's trade enforcement activities reduce risk of noncompliance and focus efforts on high-risk imports, according to CBP. For example, CBP conducts targeting of goods, conducts audits and verifications of importers, seizes prohibited goods, collects duties, and assesses penalties. However, CBP cannot assess the effectiveness of its activities without developing performance targets as suggested by leading practices for managing for results.

Over the past 5 fiscal years, CBP generally has not met the minimum staffing levels set by Congress for four of nine positions that perform customs revenue functions, and it generally has not met the optimal staffing level targets identified by the agency for these positions. Staffing shortfalls can impact CBP's ability to enforce trade effectively, for example, by leading to reduced compliance audits and decreased cargo inspections, according to CBP officials. CBP cited several challenges to filling staffing gaps, including that hiring for trade positions is not an agency-wide priority. Contrary to leading practices in human capital management, CBP has not articulated how it plans to reach its staffing targets for trade positions over the long term, generally conducting its hiring on an ad hoc basis.

Supply Chain Security: CBP Needs to Enforce Compliance and Assess the Effectiveness of the Importer Security Filing and Additional Carrier Requirements

Number: GAO-17-650
Date: 7/20/2017
Summary: Through the Importer Security Filing (ISF) and Additional Carrier Requirements (the ISF rule), CBP requires importers to submit ISFs and vessel carriers to submit vessel stow plans and container status messages (CSM). Submission rates for ISF-10s—required for cargo destined for the United States—increased from about 95 percent in 2012 to 99 percent in 2015. Submission rates for ISF-5s—required for cargo transiting but not destined for the United States—ranged from about 68 to 80 percent. To increase ISF-5 submission rates, CBP published a Notice of Proposed Rulemaking in July 2016 to clarify the party responsible for submitting the ISF-5. GAO could not determine submission rates for vessel stow plans, which depict the position of each cargo container on a vessel, because CBP calculates stow plan submission rates on a daily basis, but not comprehensively over time. CBP officials noted, though, that compliance overall is likely nearly 100 percent because Advance Targeting Units (ATU), responsible for identifying high-risk shipments, contact carriers if they have not received stow plans. GAO also could not determine submission rates for CSMs, which report container movements and status changes, because CBP does not have access to carriers' private data systems to know the number of CSMs it should receive. CBP targeters noted that they may become aware that CSMs have not been sent based on other information sources they review.

CBP has taken actions to enforce ISF and stow plan submissions, but has not enforced CSM submissions or assessed the effects of its enforcement actions on compliance at the port level.

ATUs enforce ISF and vessel stow plan compliance by using ISF holds, which prevent cargo from leaving ports, and issuing liquidated damages claims. CBP has not enforced CSM submissions because of the high volume it receives and lack of visibility into carriers' private data systems. However, when CBP targeters become aware that CSMs have not been received based on reviewing other information sources, taking enforcement actions could provide an incentive for carriers to submit all CSMs and help targeters better identify high-risk cargo. GAO's enforcement data analysis shows that ATUs used varying methods to enforce the ISF rule and that ports' ISF-10 submission rates varied. By assessing the effects of its enforcement strategies at the port level, CBP could better ensure it maximizes compliance with the rule.

CBP officials stated that ISF rule data have improved their ability to identify high-risk cargo shipments, but CBP could collect additional performance information to better evaluate program effectiveness. Evaluating the direct impact of ISF rule data in assessing shipment risk is difficult; however, GAO identified examples of how CBP could better assess the ISF program's effectiveness. For example, CBP could track the number of containers not listed on a manifest—which could pose a security risk—it identifies through reviewing vessel stow plans. Collecting this type of additional performance information could help CBP better assess whether the ISF program is improving its ability to identify high-risk shipments.

Southwest Border: Additional Actions Needed to Strengthen Management and Assess Effectiveness of Land-based Surveillance Technology

Number: GAO-17-765T
Date: 7/25/2017
Summary: CBP has made progress deploying surveillance technology along the southwest U.S. border under its 2011 Arizona Technology Plan (ATP) and 2014 Southwest Border Technology Plan. The ATP called for deployment of a mix of radars, sensors, and cameras in Arizona, and the 2014 Plan incorporates the ATP and includes deployments to the rest of the southwest border, beginning with areas in Texas and California. As of July 2017, CBP completed deployment of select technologies to areas in Arizona, Texas, and California. For example, CBP deployed all planned Remote Video Surveillance Systems (RVSS) and Mobile Surveillance Capability (MSC) systems, and 15 of 53 Integrated Fixed Tower (IFT) systems to Arizona. CBP also deployed all planned MSC systems to Texas and California and completed contract negotiations to deploy RVSS to Texas.

CBP has made progress implementing some, but not all of GAO's recommendations related to managing deployments of its technology programs. In 2014, GAO assessed CBP's implementation of the ATP and recommended that CBP: (1) apply scheduling best practices; (2) develop an integrated schedule; and (3) verify cost estimates for the technology programs. DHS concurred with some, but not all of the recommendations and has taken actions to address some of them, such as applying best practices when updating schedules, but has not taken action to address others, such as developing an integrated master schedule and verifying cost estimates with independent estimates for the IFT program. GAO continues to believe that applying schedule and cost estimating best practices could better position CBP to strengthen its management efforts of these programs.

CBP has also made progress toward assessing performance of surveillance technologies. GAO reported in 2014 that CBP identified some mission benefits, such as improved situational awareness and agent safety, but had not developed key attributes for performance metrics for all technologies, as GAO recommended (and CBP concurred) in 2011. GAO has ongoing work examining DHS's technology deployments and efforts to assess technology performance, which GAO plans to report on later this year.

Foreign Trade Zones: CBP Should Strengthen Its Ability to Assess and Respond to Compliance Risks across the Program

Number: GAO-17-649
Date: 7/27/2017
Summary: The Foreign Trade Zones (FTZ) program provides a range of financial benefits to companies operating FTZs by allowing them to reduce, eliminate, or defer duty payments on goods manufactured or stored in FTZs before they enter U.S. commerce or are exported. FTZs are secure areas located throughout the United States that are treated as outside U.S. customs territory for duty assessments and other customs entry procedures. Companies using FTZs may be warehouse distributors or manufacturers. A manufacturer, for example, that admits foreign components into the FTZ can pay the duty rate on either the foreign components or the final product, whichever is lower—resulting in reduced or eliminated duty payments. Distributors can also benefit by storing goods in FTZs indefinitely and thereby deferring duty payments until the goods enter U.S. commerce. In 2016, CBP collected about $3 billion in duties from FTZs.

While FTZs were created to provide public benefits, little is known about FTZs' economic impact. For example, few economic studies have focused on FTZs, and those that have do not quantify FTZs' economic impacts. In addition, these studies do not address the question of what the economic activity, such as employment, would have been in the absence of companies having FTZ status.

CBP has not assessed compliance risks across the FTZ program, and its methods for collecting compliance and enforcement data impair its ability to assess and respond to program-wide risks. While CBP regularly conducts compliance reviews of individual FTZ operators to ensure compliance with U.S. customs laws and regulations, it does not centrally compile FTZ compliance and enforcement information to analyze and respond to compliance and internal control risks across the program. Federal internal control standards state that management should obtain relevant data and assess and respond to identified risks associated with achieving agency goals. Without a program-wide assessment of the frequency and significance of problems identified during compliance reviews, risk levels determined, and enforcement actions taken, CBP cannot verify its assertion that the FTZ program is at low risk of noncompliance. Incorrect determinations about program risk level may impact program effectiveness and revenue collection for the FTZ program, which accounted for approximately 11 percent of U.S. imports in 2015.

International Mail Security: Costs and Benefits of Using Electronic Data to Screen Mail Need to Be Assessed

Number: GAO-17-606
Date: 8/2/2017
Summary: Express consignment operators (like FedEx and DHL) and the U.S. Postal Service (USPS) work with U.S. Customs and Border Protection to inspect inbound international express cargo and mail. Express consignment operators are required to provide "electronic advance data" (EAD)—such as the shipper's and recipient's name and address—for all inbound express cargo. CBP uses this information to target inspections. USPS is not required to provide this information to CBP. Nonetheless, as of March 2017, advance data are unavailable for roughly half of inbound international mail. Although USPS and CBP have two pilot programs under way to target mail for inspection based on EAD, they have not established specific and measureable goals and therefore lack the performance targets needed to evaluate the effectiveness of the pilots. Without these performance targets, USPS and CBP are unable to make well-informed decisions about the possible expansion of these pilots in the future. While USPS officials reported in November of 2016 that they planned to expand one of the pilots, CBP officials stated that the pilot was not ready for expansion because of USPS's inability to provide 100 percent of targeted mail to CBP for inspection. USPS stated that it is working to address challenges related to identifying targeted mail within sacks containing hundreds of individual pieces of mail.

Options for collecting EAD include negotiating agreements with foreign postal operators and legally requiring EAD, but the costs and benefits of using EAD to target mail for inspection are unclear. USPS and CBP officials stated that having EAD to target mail for inspection could result in saving time and resources and increase the percentage of inspections that identify threatening items. However, USPS has not calculated the cost of collecting EAD from countries with which it has data-sharing agreements, and neither USPS nor CBP has collected the necessary information to determine the extent to which the use of EAD would provide benefits relative to current methods of choosing mail for inspection. For example, CBP has collected data on the rate of seizures per inspection for current pilot programs, but it has not collected comparable data for other screening methods it uses to target mail for inspection. As such, USPS and CBP risk spending resources on efforts that may not increase the security of inbound international mail or that may not result in sufficient improvement to justify the costs.

International Mail Security: CBP and USPS Should Assess Costs and Benefits of Using Electronic Advance Data

Number: GAO-17-796T
Date: 9/7/2017
Summary: CBP is the primary federal agency tasked with targeting and inspecting inbound international items and seizing illegal goods, including illegal or inadmissible drugs and merchandise. As mail and express cargo arrive in the United States, both the U.S. Postal Service (USPS) and express consignment operators (such as FedEx and DHL) provide items to CBP for inspection. However, unlike express consignment operators, USPS is not currently required to provide CBP with electronic advance data (EAD), such as the shipper's and recipient's name and address, for inbound international mail and does not have control over mail prior to its arrival in the

United States. Thus, USPS relies on foreign postal operators to collect and provide EAD voluntarily or by mutual agreement.

In 2014 and 2015, USPS and CBP initiated two pilot programs at the New York International Service Center (ISC) to target certain mail for inspection using some of the EAD obtained under data-sharing agreements with foreign postal operators. Under the pilots, CBP uses EAD to target a small number of pieces of mail each day. According to USPS officials, when USPS employees scan either individual targeted pieces or larger sacks containing this targeted mail, they are alerted that CBP has targeted the item and set the item or sack aside for inspection. According to USPS and CBP, USPS has been unable to provide some targeted mail for inspection because locating targeted mail once it arrives at an ISC has been a challenge. Since the pilots began, USPS has provided CBP with about 82 percent of targeted mail for one pilot, and about 58 percent of targeted mail for the other. However, while USPS and CBP have collected some performance information for these pilots (including the percentage of targeted mail provided for inspection), this information is not linked to a specific performance target agreed upon by USPS and CBP--such as a specific percentage of targeted mail provided to CBP for inspection. Further, the agencies have not conducted an analysis to determine if the pilot programs are achieving desired outcomes. Because CBP and USPS lack clear performance goals for these pilots, they risk spending additional time and resources expanding them prior to fully assessing the pilots' success or failure.

In our report we found that the costs and benefits of using EAD to target mail for inspection are unclear. For example, according to USPS and CBP officials, increasing the use of EAD to target mail for inspection may have benefits, such as reducing time and resources needed for the screening process--potentially decreasing costs--and may increase the security of inbound mail. However, the costs of collecting and implementing the use of EAD are not yet known, and neither USPS nor CPB currently collect the data necessary to know whether using EAD might increase the security of inbound mail or decrease the time and costs associated with screening. For example, CBP has collected data on the percentage of inspections resulting in a seizure for mail inspected as a result of targeting in the pilot programs at the New York ISC. However, CBP does not collect comparable data for seizures resulting from inspections conducted based on current methods of choosing mail for inspection. In light of the challenges that collecting and using these data present, it is important that CBP and USPS carefully consider actions to enhance inbound international mail security to avoid wasting time and money on potentially ineffective and costly endeavors.

DHS OIG Reports

Review of U.S. Customs and Border Protection's Fiscal Year 2016 Drug Control Performance Summary Report

Number: OIG-17-28
Date: 2/7/2017
Summary: According to independent public accounting assessment, it was determined that CBP's FY 2016 Drug Control Performance Summary Report was reliable and in compliance with requirements of the Office of National Drug Control Policy Circular: Accounting of Drug Control Funding and Performance Summary, dated January 18, 2013.

CBP makes the following assertions:

(1) Performance reporting system is appropriate and data within these systems is accurately maintained and reliable, and properly applied to generate the most recent performance data available for the FY 2016 performance period;

(2) Explanations for not meeting performance targets are reasonable and performance targets in Fiscal Year (FY) 2016 were met for three of four measures and the explanation for not meeting one of the performance targets is reasonable;

(3) Methodology to establish performance targets is reasonable and consistently applied. The methodology described for establishing performance measure targets is based on professional judgment of subject matter experts with many years of experience in the field.

(4) Adequate performance measures exist for all significant drug control activities -CBP has established at least one performance measure for each Drug Control Decision Unit, which considers the intended purpose of the National Drug Control Program Activity. It was noted in the OIG Report 17-09, *DHS Drug Interdiction Efforts Need Improvement*, the performance measures reported for CBP's Drug Control Decision Units are not adequate. Three of the four measures were determined to be process based rather than outcome-based, and two of the four measures were found to not be sufficiently relevant to counterdrug activities. On September 26, 2016, ONDCP published a Supply Reduction Strategic Outcomes framework to provide a comprehensive and integrated perspective on strategic level changes across the spectrum of the drug supply train and associated impacts on society. Several DHS outcome-based performance measures are included in the framework, and the Department is working with ONDCP to ensure the right measures are in place to support assessment of strategic outcomes. As a follow-on activity, CBP will work with the Department on the development of new measures for fiscal year 201 8, as needed. CBP did determine that the FY2016 performance measures for all significant drug control activities did not require material modification.

DHS Drug Interdiction Efforts Need Improvement

Number: OIG-17-09
Date: 11/8/2016
Summary: DHS leads the Nation's drug interdiction efforts through a multi-component-led approach, including the U.S. Coast Guard, CBP, and ICE. DHS's Office of Policy coordinates strategy and policy within the Department and identifies resource gaps in Department drug interdiction actions.

OIG reported that the Office of National Drug Control Policy (ONDCP) found DHS's oversight of its drug interdiction efforts did not align with ONDCP's National Drug Control Strategy. Specifically, the Department did not: (1) report drug seizures and drug interdiction resource hours to ONDCP, and (2) ensure its components developed and implemented adequate performance measures to assess drug interdiction activities. As a result, DHS could not ensure its drug interdiction efforts met required national drug control outcomes nor accurately assess the impact of the approximately $4.2 billion it spends annually on drug control activities. DHS and ONDCP

recognize that performance measures need improvements and have taken steps to address these improvements.

OIG also identified potential issue that could affect the Department's ability to accurately report the total amount of drugs it seizes during component operations. During OIG's interviews with stakeholders, component officials noted the potential for duplication when recording drug seizures made by more than one agency. As a result, OIG conducted limited testing on drug seizure data to determine whether components duplicated drug seizure data within their systems. OIG found duplication in data recording when CBP and ICE are part of joint operations. Components track and report their drug seizure data using individual systems of record. OIG reviewed examples of components' internal tracking on drug seizure data and found 437 cases of duplication in CBP and ICE data. Combining these duplicated drug seizures could give the perception that DHS is interdicting more drugs than it is.

OIG noted that DHS lacks a centralized authority responsible for its counterdrug activities and without effective performance measures or consistent drug seizure recording and reporting, DHS cannot ensure it is supporting the Federal Government counterdrug priorities to its full potential.

Management Alert - Security and Safety Concerns at Border Patrol Stations in the Tucson Sector (Redacted)

Number: OIG-17-115-MA
Date: 9/29/2017
Summary: In April 2017, OIG conducted unannounced spot inspections of Border Patrol stations and the Tucson Coordination Center (TCC) in the Tucson Sector in Arizona. During these unannounced inspections, OIG toured the facilities, reviewed documentation from previous inspections, and interviewed Border Patrol staff. This report describes physical security issues OIG identified that pose an immediate threat to Border Patrol agents, assets, and operations at stations within the Tucson Sector, as well as security issues related to cameras and access at two other Border Patrol stations and the TCC in the Tucson Sector.

OIG found, two facilities that had vulnerable outdoor storage containers secured with padlocks that could be easily opened with common bolt cutters. Container tops and walls could also easily be compromised with a blow torch or other widely available tools. The containers we inspected held ammunition; small arms; riot control explosives; proprietary surveillance equipment; seized drugs; and sensitive hardcopy prosecution, investigation, and personnel documents.

OIG also found that one station's 8-foot high perimeter wall has inadequate camera coverage and allows public access to the full perimeter and visibility of storage containers, as well as seized and Government vehicles. Further, poor outdoor lighting hinders night camera surveillance. At another station exterior cameras are inoperable, and the surrounding 6-foot high chain link fence allows public access to the full perimeter and visibility of Government vehicles, storage containers, structures, a fuel storage tank, and operations. OIG noted other security issues related to camera visibility at three additional stations. Specifically, at two facilities, control room monitor displays that cover detainee cells were either not functional, too blurry to provide detail, or too small to be effective.

CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations

Number: OIG-17-114
Date: 9/28/2017
Summary: OIG found that CBP's information technology (IT) systems and infrastructure did not fully support its border security objective of preventing the entry of inadmissible aliens to the country. The slow performance of a critical pre-screening system greatly reduced Office of Field Operations officers' ability to identify any passengers who may represent concerns, including national security threats. Additionally, incoming passenger screening at U.S. international airports was hampered by frequent system outages that created passenger delays and public safety risks. The outages required that CBP officers rely on backup systems that weakened the screening process, leading to officers potentially being unable to identify travelers that may be attempting to enter the United States with harmful intent. IT systems and infrastructure also did not fully support Border Patrol and Air and Marine Operations border security activities between ports of entry. Poor systems performance and network instability hampered these CBP operations nationwide. This resulted in excessive processing backlogs and agents' inability to meet court deadlines for submitting potential alien criminal prosecution cases. Also, frequent network outages hindered air and marine surveillance operations, greatly reducing the situational awareness needed to detect inadmissible aliens and cargo approaching U.S. borders. CBP has not yet addressed these long-standing IT systems and infrastructure challenges, due in part to ongoing budget constraints.

CBP's Border Security Efforts – An Analysis of Southwest Border Security Between the Ports of Entry

Number: OIG-17-39
Date: 2/27/2017
Summary: CBP guards nearly 2,000 miles of U.S. land border with Mexico, seeking to deter, detect, and interdict illegal entry of people and contraband into the United States while facilitating lawful travel and trade. CBP also enforces applicable U.S. laws, including those pertaining to illegal immigration, narcotics smuggling, and illegal importation. Within CBP, the Border Patrol uses its $3.8 billion operating budget to secure areas between ports of entry. According to CBP, the Border Patrol's more than 21,000 agents accomplish this mission using surveillance, sensor alarms and aircraft sightings, and interpreting and following tracks.

OIG's review of pervious audit and research reports on southwest border security issued by DHS OIG, GAO, and CRS since 2003, concluded that CBP has instituted many border security programs and operations that align with the 1993 Sandia National Laboratories (Sandia) study recommendations. However, OIG's review and analysis of these reports also highlighted some continuing challenges to CBP's efforts to secure the southwest border. In particular, CBP does not measure the effectiveness of its programs and operations well; therefore, it continues to invest in programs and act without the benefit of the feedback needed to help ensure it uses resources wisely and improves border security. CBP also faces program management challenges in planning, resource allocation, infrastructure and technology acquisition, and overall efficiency. Finally, OIG noted that coordination and communication with both internal and external stakeholders could be improved.

DHS' Joint Task Forces

Number: OIG-17-100
Date: 8/10/2017
Summary: In 2014, DHS created three pilot Joint Task Forces (JTF) to address challenges along the Southern Border. In January 2015, JTF-Investigations developed a process for determining the top criminal networks impacting homeland security and conducting National Case Coordination to eliminate them. This process supports JTF-East and JTF-West. From May to August of 2016, JTF-West conducted Operation "All In" to disrupt human smuggling activities that affect the Southern Border. According to DHS, due to the success of this operation, the Secretary approved it as an "open ended, steady-state enforcement effort." Finally, in fiscal year 2017 JTF-East supported Operation "Caribbean Guard," which resulted in migrant arrests, drug interdiction, and seized currency.

According to JTF leaders, operational effectiveness and efficiency has increased; staff morale has improved; and components have successfully worked together to promote information sharing and communication. However, OIG found that although the JTFs are a step forward for DHS, they face challenges, including a need for dedicated funding and outcome-based performance measures. Without dedicated funding, the JTFs rely on components that may have competing or conflicting priorities. Without performance metrics, the JTFs cannot show the value they add to homeland security operations.

Special Report: Challenges Facing DHS in Its Attempt to Hire 15,000 Border Patrol Agents and Immigration Officers

Number: OIG-17-98-SR
Date: 7/27/2017
Summary: On January 25, 2017, the President issued two Executive Orders directing the Department of Homeland Security to hire an additional 5,000 Border Patrol Agents and 10,000 Immigration Officers.

OIG found that although DHS has established plans and initiated actions to begin the hiring surge, in recent years the Department and its components have encountered difficulties related to long hire times, proper allocation of staff, and the supply of human resources. OIG noted that both CBP and ICE need proper workforce planning to ensure correct staffing levels, ratios, and placements, and to guide targeted recruitment campaigns.

In addition, OIG found that both CBP and ICE needed a comprehensive workforce staffing model and must determine operational needs and develop deployment strategies. In April 2016, OIG found that CBP did not: 1) properly assess the major duties its criminal investigators perform, 2) conduct an adequate analysis of its staffing needs, or 3) develop performance measures to assess the effectiveness of its investigative operations. Without a comprehensive process and analysis, CBP may have improperly spent approximately $3.1 million and as much as $22.6 million over 5 years for questionable Law Enforcement Availability Pay. Improving data reliability and strengthening internal controls over the Workload Staffing Model would ensure that CBP is efficiently allocating staffing resources and submitting budget requests that accurately reflect staffing needs.

OIG also found due to lack of an effective workforce deployment strategy, the deportation workloads in various ICE field offices was uneven, resulting in some deportation officers being overwhelmed with their caseloads. OIG also noted the need for significant enhancements to recruitment and retention to attract qualified candidates.

Lessons Learned from Prior Reports on CBP's SBI and Acquisitions Related to Securing our Border

Number: OIG-17-70-SR
Date: 6/12/2017
Summary: On January 25, 2017, the President signed Executive Order No.13767, Border Security and Immigration Enforcement Improvements. The Executive Order directed executive departments and agencies to deploy all lawful means to secure the Nation's southern border through the immediate construction of a physical wall, monitored and supported by adequate personnel so as to prevent illegal immigration, drug, and human trafficking, and acts of terrorism. CBP currently faces an aggressive implementation schedule to satisfy the Executive Order requirement. CBP is working on an acquisition plan while simultaneously preparing a solicitation for the design and build of a southern border wall.

OIG noted that CBP must be mindful of the lessons learned related to an aggressively scheduled acquisition in order to protect taxpayer dollars associated with the acquisition of the construction of a southern border wall. OIG noted that CBP needs to ensure operational requirements are will defined and validated as prior reports identified that CBP did not have defined and validated operational requirements resulting in unachievable performance.

OIG also reported that in 2011, the GAO reported CBP did not document the analysis justifying the specific types, quantities, and deployment locations of border surveillance technologies proposed in the Arizona Border Surveillance Technology Plan (Plan). In addition, CBP's life cycle cost estimate for the Plan did not sufficiently meet characteristics of a high-quality cost estimate, such as credibility, because it did not identify a level of confidence or quantify the impact of risk.

OIG points out that acquisition planning is one of the most important phases in the acquisition process and that failure to adequately plan may result in missed milestones and poorly defined and documented requirements. This will further hampers adequate definition of customer needs in the contract solicitation.

CBP Continues to Improve its Ethics and Integrity Training, but Further Improvements are Needed

Number: OIG-17-60
Date: 5/31/2017
Summary: CBP has made improvements to, and continues to develop, its ethics and integrity training for officers and agents. It tracks training completion, and has begun to measure and assess training effectiveness. However, the Performance and Learning Management System used to track training completion needs improvement. Also, locally developed training content on ethics and integrity varies by location and operating environment, and CBP does not maintain a repository or

any formal process for the field to share locally developed information. As a result, CBP misses valuable opportunities to deliver consistent high-quality ethics and integrity training courses across multiple operating environments and components.

Finally, CBP has not effectively communicated or followed up with the field on its overall Integrity and Personal Accountability Strategy. One purpose of the strategy is to ensure that ethics and integrity training is provided for all CBP employees. More broadly, the strategy aims to promote a culture of integrity and accountability by increasing awareness through messaging, training, and enhanced communication. If employees have not received or do not understand the importance of the integrity strategy, CBP cannot succeed in achieving this important initiative.

Management Alert - CBP Spends Millions Conducting Polygraph Examinations on Unsuitable Applicants

Number: OIG-17-99-MA
Date: 8/4/2017
Summary: CBP administered polygraph examinations to applicants who previously provided disqualifying information on employment documents or during the pre-test interview. This occurred because CBP's process did not stop, and is not sufficient to prevent, unsuitable applicants from continuing through the polygraph examination. Specifically, CBP: 1) does not have a step, such as the security interview, to identify and remove applicants who provide disqualifying information well before they are scheduled to appear for a polygraph examination; 2) did not require examiners to consistently use the on-call adjudicator process until May 2017; and 3) does not end the exam immediately after an unsuitable determination. As a result, CBP administered polygraph examinations to individuals who provided disqualifying information during the polygraph pretest interview. We estimated CBP spent about $5.1 million completing more than 2,300 polygraphs to applicants with significant pre-test admissions of wrongdoing between FYs 2013 and 2016. CBP could not hire these applicants regardless of their polygraph results.

OIG found that subjecting unsuitable applicants to the polygraph examination has a direct impact on the high failure rate of the polygraph program and limits CBP's capability to address its short- and long-term hiring needs. Given that DHS has committed to increase staffing, CBP should put its funds to better use by focusing its polygraph resources on applicants with the best chance of making it through the hiring process. Not doing so slows the process for qualified applicants, wastes polygraph resources on unsuitable applicants, and will make it more difficult to achieve its hiring goal.

If CBP implemented a security interview and improved utilization of the adjudicative process, it could put its funds to better use by focusing on applicants with the best chance of making it through the hiring process. Not doing so slows the process for qualified applicants; wastes polygraph resources on unsuitable applicants; and will make it more difficult for CBP to achieve its hiring goals.

Departmental Management and Operations (DMO)

GAO Reports

Homeland Security Acquisitions: Joint Requirements Council's Initial Approach Is Generally Sound and It Is Developing a Process to Inform Investment Priorities

Number: GAO-17-171
Date: 10/24/2016
Summary: In 2003, DHS established a Joint Requirements Council to review and prioritize requirements across the department's components—such as the U.S. Coast Guard and U.S. Customs and Border Protection. However, due to a lack of senior management involvement, it became inactive. Over a decade later and after a 2008 GAO recommendation that the JRC be reinstated, the Secretary of Homeland Security directed the creation of a new JRC in June 2014. GAO was asked to review the organization and activities of the current JRC. This report addresses, among other things, the extent to which the JRC: (1) has a structure and management approach consistent with key practices; and (2) has begun reviewing and validating capability and requirements documents and informing DHS investment priorities.

Department of Homeland Security: Important Progress Made, but More Work Remains to Strengthen Management Functions

Number: GAO-17-409T
Date: 2/17/2017
Summary: GAO has regularly reported on government operations identified as high-risk because of their increased vulnerability to fraud, waste, abuse, and mismanagement, or the need for transformation to address economy, efficiency, or effectiveness challenges. In 2003, GAO designated implementing and transforming DHS as high-risk because DHS had to transform 22 agencies into one department, and failure to address associated risks could have serious consequences for U.S. national and economic security. Challenges remain for DHS across its range of missions, but it has made considerable progress. As a result, in its 2013 high-risk update, GAO narrowed the scope of the high-risk area to strengthening and integrating DHS management functions (human capital, acquisition, financial, and information technology).

This statement discusses, among other things, DHS's progress and actions remaining in strengthening and integrating its management functions. This statement is based on GAO's 2017 high-risk update and reports and testimonies from September 2011 through mid-February 2017. Among other things, GAO analyzed DHS strategies and interviewed DHS officials.

Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts

Number: GAO-17-300
Date: 4/6/2017
Summary: Violent extremism—generally defined as ideologically, religious, or politically-motivated acts of violence—has been perpetrated in the United States by white supremacists, anti-

government groups, and radical Islamist entities, among others. In 2011, the U.S. government developed a national strategy and Strategic Implementation Plan for CVE aimed at providing information and resources to communities. In 2016, an interagency CVE Task Force led by DHS and DOJ was created to coordinate CVE efforts.

GAO was asked to review domestic federal CVE efforts. This report addresses the extent to which (1) DHS, DOJ, and other key stakeholders tasked with CVE in the United States have implemented the 2011 SIP and (2) the federal government has developed a strategy to implement CVE activities, and the CVE Task Force has assessed progress. GAO assessed the status of activities in the 2011 SIP; interviewed officials from agencies leading CVE efforts and a non-generalizable group of community-based entities selected from cities with CVE frameworks; and compared Task Force activities to selected best practices for multi- agency efforts.

Homeland Security Acquisitions: Earlier Requirements Definition and Clear Documentation of Key Decisions Could Facilitate Ongoing Progress

Number: GAO-17-346SP
Date: 4/6/2017
Summary: In fiscal year 2016, DHS planned to invest about $7 billion in major acquisitions. DHS's acquisition activities are on GAO's High Risk List, in part due to program management, requirements, and funding issues. The Explanatory Statement accompanying the DHS appropriations Act, 2015 included a provision for GAO to review DHS's major acquisitions. This report, GAO's third annual review, addresses the extent to which (1) DHS's major acquisition programs are on track to meet schedule and cost goals, (2) these programs are meeting KPPs, and (3) DHS has strengthened implementation of its acquisition policy. GAO assessed DHS's 15 largest acquisition programs that were in the process of obtaining new capabilities as of May 2016, and 11 additional programs that GAO or DHS identified were at risk of poor outcomes. For all 26 programs, GAO reviewed key documentation, assessed performance against baselines established since DHS's 2008 acquisition policy, and met with program officials. GAO also met with DHS acquisition officials and assessed DHS's policies and practices against GAO acquisition best practices and federal internal control standards.

Homeland Security Acquisitions: Identifying All Non-Major Acquisitions Would Advance Ongoing Efforts to Improve Management

Number: GAO-17-396
Date: 4/13/2017
Summary: Each year, DHS acquires a wide array of systems intended to help its component agencies execute their many critical missions. GAO has previously reported that DHS's process for managing its major acquisitions is maturing. However, non-major acquisitions (generally those with cost estimates of less than $300 million) are managed by DHS's component agencies and have not received as much oversight. Recently GAO reported on a non-major acquisition that was executed poorly, limiting DHS's ability to address human capital weaknesses.

Homeland Security: Progress Made to Implement IT Reform, but Additional Chief Information Officer Involvement Needed

Number: GAO-17-284
Date: 5/18/2017
Summary: In 2014, Congress enacted IT reform legislation, referred to as the Federal Information Technology Reform Act (FITARA), which includes provisions related to seven areas of IT acquisition management. In 2015, OMB released FITARA implementation guidance that outlined agency CIO responsibilities and required agencies to develop action plans for implementing the guidance. This report examines, among other things, the extent to which DHS has implemented selected action plans and the key challenges that DHS has faced in implementing selected FITARA provisions.

DHS Financial Management: Better Use of Best Practices Could Help Manage System Modernization Project Risks

Number: GAO-17-799
Date: 9/26/2017
Summary: To help address long-standing financial management system deficiencies, DHS initiated its TRIO project which has focused on migrating three of its components—U.S. Coast Guard, Transportation Security Administration (TSA), and Domestic Nuclear Detection Office (DNDO), to a modernized financial management system provided by the Interior Business Center (IBC), an OMB-designated, federal shared service provider (SSP). House Report Number 3128 included a provision for GAO to assess the risks of DHS using IBC in connection with its modernization efforts. This report examines (1) the extent to which DHS and the TRIO components followed best practices in analyzing alternatives, and the key factors, metrics, and processes used in their choice of a modernized financial management system; (2) the extent to which DHS managed the risks of using IBC for its TRIO project consistent with risk management best practices; and (3) the key factors and challenges that have impacted the TRIO project and DHS's plans for completing remaining key priorities. GAO interviewed key officials, reviewed relevant documents, and determined whether DHS followed best practices identified by GAO as necessary characteristics of a reliable, high-quality AOA process and other risk management best practices

DHS Financial Management: Improved Use of Best Practices Could Help Manage System Modernization Project Risks

Number: GAO-17-803T
Date: 9/26/2017
Summary: In 2013, the OMB issued direction to agencies to consider federal Shared Service Providers (SSP) as part of their alternatives analysis. Subsequently, in May 2014, OMB and the Department of the Treasury (Treasury) designated Interior Business Center (IBC) as one of four federal SSPs for financial management to provide core accounting and other services to federal agencies. In addition, Treasury's Office of Financial Innovation and Transformation's (FIT) responsibilities related to the governance and oversight of federal SSPs were subsequently transferred to the Unified Shared Services Management office (USSM) after USSM was established in October 2015 as an entity within the General Services Administration.

This statement summarizes our report that examined (1) the extent to which DHS and Domestic Nuclear Detection Office (DNDO), Transportation Security Administration (TSA), and U.S. Coast Guard, or "the TRIO components," followed best practices in analyzing alternatives, and the key factors, metrics, and processes used in their choice of a modernized financial management system; (2) the extent to which DHS managed the risks of using IBC for its TRIO project consistent with risk management best practices; and (3) the key factors and challenges that have impacted the TRIO project and DHS's plans for completing the remaining key priorities.

Federal Programs: Information Architecture Offers a Potential Approach for Development of an Inventory

Number: GAO-17-739
Date: 9/29/2017
Summary: Each year the federal government spends trillions of dollars through dozens of agencies and thousands of federal programs. Given its sheer size and scope, providing a clear and complete picture of what the federal government does and how much it costs has been a challenge in the absence of a comprehensive resource describing these programs. The GPRA Modernization Act of 2010 (GPRAMA) requires the Office of Management and Budget (OMB) to present a coherent picture of all federal programs by making information about each program available on a website to enhance the transparency of federal government programs.

Congress included a provision in GPRAMA for GAO to review the implementation of the act. GAO has chosen to conduct this study now because OMB has not yet developed an inventory that meets GPRAMA requirements. For this report, GAO addresses how one potential approach for organizing and structuring information—the principles and practices of information architecture—can be applied to develop a useful federal program inventory. To present illustrative examples of what programs and program information could be included in an inventory, GAO examined budget, performance, and other resources that could be used to develop an inventory. These examples were also used to illustrate the potential content and structure of an inventory and to identify any challenges

A useful federal program inventory would consist of all programs identified, information about each program, and the organizational structure of the programs and information about them. The principles and practices of information architecture—a discipline focused on organizing and structuring information—offer an approach for developing such an inventory to support a variety of uses, including increased transparency for federal programs. GAO identified a series of iterative steps that can be used to develop an inventory and potential benefits of following this approach. GAO also identified potential challenges agencies may face in developing a full program inventory.

Critical Infrastructure Protection: Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts

Number: GAO-17-182
Date: 2/7/2017
Summary: The six selected federally-administered critical infrastructure access control efforts GAO reviewed generally followed similar screening and credentialing processes. Each of these

efforts applies to a different type of infrastructure. For example, the Transportation Security Administration's Transportation Worker Identification Credential controls access to ports, the Department of Defense (DOD) Common Access Card controls access to military installations, and the Nuclear Regulatory Commission (NRC) regulates access to commercial nuclear power plants. GAO found that selected characteristics, such as whether a federal agency or another party has responsibility for vetting or what types of prior criminal offenses might disqualify applicants, varied across these access control efforts. In addition, these access control efforts generally affect two groups of stakeholders—users and operators—differently depending on their specific roles and interests. Users are individuals who require access to critical infrastructure as an essential function of their job; while, operators own or manage facilities, such as airports and chemical facilities. Regardless of infrastructure type, users and operators that GAO interviewed reported some common factors that can present challenges in their use of these access controls. For example, both users and operators reported that applicants requiring access to similar types of infrastructure or facilities may be required to submit the same background information multiple times, which can be costly and inefficient.

The Department of Homeland Security (DHS) relies on partnership models to support collaboration efforts among federal and nonfederal critical infrastructure stakeholders, but has not taken actions to harmonize federally-administered access control efforts across critical infrastructure sectors. According to DHS officials, these partnerships have not explored harmonization of access control efforts across sectors, because this has not been raised as a key issue by the members and because DHS does not have a dedicated forum that would engage user groups in exploring these issues and identifying potential solutions. DHS's partnership models offer a mechanism by which DHS and its partners can explore the challenges users and operators may encounter and determine opportunities for harmonizing the screening and credentialing processes to address these challenges.

DHS's Screening Coordination Office (SCO) has taken actions to support harmonization across DHS access control efforts, but it has not updated its goals and objectives to help guide progress toward the department's broader strategic framework for harmonization. SCO's strategic framework is based on two screening and credentialing policy documents—the 2006 Credentialing Initiative Report and 2008 Credentialing Framework Initiative. According to SCO officials, they continue to rely on these documents to provide their office with a high-level strategic approach, but GAO found that the goals and objectives outlined in the two documents are no longer current or relevant. In recent years, SCO has helped the department make progress toward its harmonization efforts by responding to and assisting with department-wide initiatives and DHS component needs, such as developing new programs or restructuring existing ones. However, without updated goals and objectives, SCO cannot ensure that it is best supporting DHS-wide screening and credentialing harmonization efforts.

Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices

Number: GAO-17-549
Date: 9/28/2017
Summary: During fiscal year 2016, federal agencies continued to experience weaknesses in protecting their information and information systems due to ineffective implementation of information security policies and practices. Most of the 24 Chief Financial Officers Act (CFO)

agencies had weaknesses in five control areas—access controls, configuration management controls, segregation of duties, contingency planning, and agency-wide security management (see figure). GAO and inspectors general (IGs) evaluations of agency information security programs, including policies and practices, determined that most agencies did not have effective information security program functions in fiscal year 2016. GAO and IGs have made hundreds of recommendations to address these security control deficiencies, but many have not yet been fully implemented.

OMB, DHS, National Institute of Standards and Technology (NIST), and IGs have ongoing and planned initiatives to support implementation of the Federal Information Security Management Act of 2002 as amended by the Federal Information Security Modernization Act of 2014 (FISMA) across the federal government. OMB, in consultation with other relevant entities, has expanded the use of a maturity model developed by the Council of the Inspectors General on Integrity and Efficiency and used to evaluate additional information security performance areas each year. However, OMB and others have not developed a plan and schedule to determine whether using the security capability maturity model will provide useful results that are consistent and comparable. Until an evaluative component is incorporated into the implementation of the maturity model, OMB will not have reasonable assurance that agency information security programs have been consistently evaluated.

DHS OIG Reports

DHS Pandemic Planning Needs Better Oversight, Training, and Execution

Number: OIG-17-02
Date: 10/12/2016
Summary: DHS has taken steps to develop a Departmental Pandemic Workforce Protection Plan intended to protect the workforce during a pandemic event. In addition, as a result of OIG recommendations, the Department has created an integrated logistics support plan for personal protective equipment. However, DHS cannot be assured that its preparedness plans can be executed effectively during a pandemic event. This review is the third in a series of audits on DHS's pandemic preparedness and response. This audit focused on whether the Department had adequate preparedness plans to continue its essential missions during a pandemic.

DHS Is Slow to Hire Law Enforcement Personnel

Number: OIG-17-05
Date: 10/31/2016
Summary: Although CBP, ICE, and the Secret Service have been able to maintain staffing levels close to the authorized number of law enforcement personnel, they continue to have significant delays in hiring. The additional steps in the hiring process for law enforcement applicants contribute to the length of time it takes to hire law enforcement officers, but the components also do not have the staff or comprehensive automated systems needed to hire personnel as efficiently as possible. Although they have taken steps to reduce the time it takes to hire law enforcement personnel, it is too early to measure the long-term effects of the Department's and the components' recent actions. The inability to hire law enforcement personnel in a timely manner may lead to

shortfalls in staffing, which can affect workforce productivity and morale, as well as potentially disrupt mission critical operations.

Specifically the OIG reviewed (1) the effectiveness of the three components in filling vacant positions; (2) the timeliness of the hiring process, including areas of delays; and (3) process improvements implemented by the three components.

Major Management and Performance Challenges Facing the Department of Homeland Security

Number: OIG-17-08
Date: 11/7/2016
Summary: Although significant progress has been made over the last 3 years, the Department continues to face long-standing, persistent challenges overseeing and managing its homeland security mission. These challenges affect every aspect of the mission, from preventing terrorism and protecting our borders and transportation systems to enforcing our immigration laws, ensuring disaster resiliency, and securing cyberspace. The Department is continually tested to work as one entity to achieve its complex mission. To better inform and assist the Department, this year we are presenting a broader picture of management challenges by highlighting those we have repeatedly identified over several years. We remain concerned about the systemic nature of these challenges, some of which span multiple Administrations and changes in Department leadership. Overcoming these challenges demands unified action; a motivated and engaged work force; rigorous, sustained management of acquisitions and grants; and secure information technology (IT) systems that protect sensitive information, all of which must be based on the management fundamentals of data collection, cost-benefit analysis, and performance measurement.

Improvements Needed to Promote DHS Progress toward Accomplishing Enterprise-wide Data Goals

Number: OIG-17-101
Date: 8/14/2017
Summary: In August 2016, DHS issued the *Enterprise Data Strategy* as a guide for managing its data as an asset. OIG performed this audit to determine the status of DHS' implementation of the data strategy and whether it is effectively coordinating component data investments to support mission accomplishment.

As of April 2017, DHS had begun implementing only 4 of 23 strategic objectives of its Enterprise Data Strategy. It had not taken steps to finalize activities, assign responsibilities, define outcomes, and establish timelines for addressing the remaining 19 objectives. DHS delayed finalizing its plans for implementing many of the strategic objectives in the data strategy until late fiscal year 2017 to avoid duplication with planning for related information sharing efforts. Finalizing the implementation plans will be essential for DHS to progress in executing its strategy for ensuring standardization, interoperability, accessibility, and inventory of its data assets department-wide.
Further, the Department faces challenges implementing the data strategy due to its broad scope and the complex coordination it entails. The Department has instituted a number of initiatives and working groups that have been effective in coordinating and monitoring data investments across components to help them achieve their respective missions. However, component officials identified a number of areas where the Department could provide additional assistance, such as furthering data integration, and

providing common tools to support DHS-wide data analysis and management. Providing the additional assistance needed to coordinate component data investments may spur Department progress toward meeting its enterprise-wide data goals.

DHS Review of Responses to Significant Freedom of Information Act Requests (Verification Review of OIG-11-67)

Number: OIG-17-116-VR
Date: 9/29/2017
Summary: Department of Homeland Security records are subject to release under the *Freedom of Information Act* (FOIA).[1] Enacted in 1966 and amended several times, Freedom of Information Act (FOIA) mandates that Federal executive branch agencies release certain information to the public upon request, unless the information falls within one of nine exemptions which protect certain interests, such as personal privacy or national security. The act also includes timetables within which Federal agencies must respond to FOIA requests. Generally, agencies must release responses to FOIA requests within 20 days, unless certain specific circumstances allow for an extension. In addition, the Department of Justice has interpreted the statute to mean that agencies may not prevent release of information simply because it is embarrassing.

OIG conducted this review in response to a June 2015 request from the Senate Committee on Homeland Security and Governmental Affairs to determine whether political appointees were involved in DHS' FOIA response process and delayed FOIA releases or inappropriately withheld information.

In March 2011, the DHS OIG issued a report, *The DHS Privacy Office Implementation of the Freedom of Information Act* (OIG-11-67), which addressed similar concerns. The report concluded that political appointees in DHS headquarters might have improperly delayed or withheld releases of information from responses to significant FOIA requests.

DHS Lacks Oversight of Component Use of Force (Redacted)

Number: OIG-17-22
Date: 1/12/2017
Summary: DHS employs approximately 80,000 federal law enforcement officers whose positions allow for the use of force as they perform their duties. Every day law enforcement officers face danger when performing their duties. These officers have very little time to assess the situation and determine the proper response when dealing with a dangerous or unpredictable situation. The officers must react to the threat or potential threat and respond with the appropriate tactics—possibly including some level of force. DHS has not done enough to minimize the risk of improper use of force by law enforcement officers. Specifically, the Department does not:

- have an office responsible for managing and overseeing component use of force Activities;
- ensure the collection and validation of component data needed to assess use of force activities, minimize risks, and take corrective actions;
- ensure use of force policies have been updated to reflect current operations and lessons learned; or

- establish consistent requirements for less lethal recurrent training and ensure training was completed as required.

Additionally, each component varies on their use of force activities. Without improvements in the management and oversight of use of force activities, the Department may increase its risk of improper use of force by law enforcement officers.

Table of Smaller Reports

Date	Number	Title
2/1/2017	OIG-17-33	Review of U.S. Coast Guard's Fiscal Year 2016 Review of U.S. Coast Guard's Fiscal Year 2016 Drug Control Performance Summary Report
2/6/2017	OIG-17-36	Independent Auditors' Report on U.S. Customs and Border Protection's Fiscal Year 2016 Consolidated Financial Statements
3/6/2017	OIG-17-43-MA	Management Alert on Issues Requiring Immediate Action at the Theo Lacy Facility in Orange, California
4/27/2017	OIG-17-52	Management Letter for the Department of Homeland Security's Fiscal Year 2016 Financial Statements Audit
4/28/2017	OIG-17-54	Information Technology Management Letter for the FY 2016 Department of Homeland Security Financial Statement Audit
5/8/2017	OIG-17-53	National Flood Insurance Program's Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
5/15/2017	OIG-17-55	Information Technology Management Letter for the FY 2016 U.S. Customs and Border Protection Financial Statement Audit
5/25/2017	OIG-17-61	Information Technology Management Letter for the United States Coast Guard Component of the FY 2016 DHS Financial Statement Audit
6/8/2017	OIG-17-63	Information Technology Management Letter for the U.S. Immigration and Customs Enforcement Component of the FY 2016 Department of Homeland Security Financial Statement Audit
6/12/2017	OIG-17-71	United States Immigration and Customs Enforcement's Management Letter for DHS' FY 2016 Financial Statements Audit
6/13/2017	OIG-17-69	Transportation Security Administration's Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
6/13/2017	OIG-17-68	Federal Law Enforcement Training Centers' Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
6/13/2017	OIG-17-64	Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2016 Department of Homeland Security Financial Statement Audit
6/14/2017	OIG-17-67	Federal Emergency Management Agency's Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
6/15/2017	OIG-17-72	Information Technology Management Letter for the United States Secret Service Component of the FY 2016 Department of Homeland Security Financial Statement Audit

Date	Number	Title
6/21/2017	OIG-17-73	Information Technology Management Letter for the Transportation Security Administration Component of the FY 2016 Department of Homeland Security Financial Statement Audit
6/22/2017	OIG-17-78	Information Technology Management Letter for the National Protection and Programs Directorate of the FY 2016 Department of Homeland Security Financial Statement Audit
6/26/2017	OIG-17-82	Science and Technology Directorate's' Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
6/26/2017	OIG-17-81	Information Technology Management Letter for the Science and Technology Directorate Component of the FY 2016 Department of Homeland Security Financial Statement Audit
6/26/2017	OIG-17-76	Information Technology Management Letter for the U.S. Citizenship and Immigration Services Component of the FY 2016 Department of Homeland Security Financial Statement Audit
6/27/2017	OIG-17-84	United States Citizenship and Immigration Services' Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
6/28/2017	OIG-17-85	Information Technology Management Letter for the Office of Financial Management and Office of the Chief Information Officer Components of the FY 2016 Department of Homeland Security Financial Statement Audit
6/28/2017	OIG-17-75	Information Technology Management Letter for the Federal Law Enforcement Training Centers Component of the FY 2016 Department of Homeland Security Financial Statement Audit
6/29/2017	OIG-17-87	United States Secret Service's Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
6/29/2017	OIG-17-86	Office of Financial Management's Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
6/30/2017	OIG-17-90	Management Letter for U.S Customs and Border Protection's Fiscal Year 2016 Consolidated Financial Statements Audit
6/30/2017	OIG-17-89	United States Coast Guard's Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
6/30/2017	OIG-17-88	Information Technology Management Letter for the Management Directorate Component of the FY 2016 Department of Homeland Security Financial Statement Audit
7/3/2017	OIG-17-92	National Protection and Programs Directorate's Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
7/7/2017	OIG-17-96	Management Directorate's Management Letter for DHS' Fiscal Year 2016 Financial Statements Audit
7/10/2017	OIG-17-94	Audit of Department of Homeland Security's Fiscal Years 2014 and 2015 Conference Spending
7/11/2017	OIG-17-45-MA	Management Alert Regarding Inspector General Access to Information (OIG 17-45-MA)

Federal Emergency Management Agency (FEMA)

GAO Reports

Emergency Communications: Improved Procurement of Land Mobile Radios Could Enhance Interoperability and Cut Costs

Number: GAO-17-12
Date: 10/5/2016
Summary: GAO surveyed found that Federal agencies generally use land mobile radio (LMR) equipment to meet their core missions, such as public safety, emergency management, or firefighting. More than two-thirds of the 57 agencies GAO surveyed reported using equipment from the same manufacturer because, for example, they believe doing so will help ensure compatibility of new LMR equipment with existing system requirements. Most agencies GAO surveyed were consistent in identifying each other as agencies with which they have or have not needed LMR interoperability over the past 5 years. Of the agencies that identified the need to communicate with each other, about two-thirds reported generally having a good or excellent level of LMR interoperability.

The use of standards-based and multi-band LMR equipment has helped to enhance interoperability among agencies, but the use of proprietary features and other factors continue to hinder interoperability. Nearly all of the agencies that GAO surveyed reported using LMR equipment that meets voluntary technical standards, which have improved interoperability. Further, almost half of these agencies reported using multiband radios, which operate on multiple public-safety radio bands, to enhance interoperability. However, agencies reported several factors continue to limit their progress in achieving interoperability with other federal agencies. These factors include the use of proprietary features and encryption in devices and limited investments in LMR systems and devices. For example, about half of the agencies surveyed reported that the use of proprietary features within LMR devices has hindered interoperability.

Almost half of the agencies GAO surveyed reported using pre-approved vendors with established prices to acquire LMR equipment, mainly through contracts sponsored by the Departments of Homeland Security and the Interior. While this approach can facilitate cost savings and interoperability, many of these agencies reported purchasing equipment through multiple agreements, a practice that can reduce these benefits. About 40 percent of agencies GAO surveyed reported using sole-source procurement or independent approaches. According to the Office of Management and Budget (OMB), in general, agencies often purchase and manage items in a fragmented and inefficient manner. This approach can result in duplication of effort, which imposes significant costs on federal agencies. OMB has directed agencies to implement "category management" as an improved way to manage spending across government for commonly purchased goods and services. This approach enables the government to leverage its purchasing power and realize cost savings. However, OMB's category management initiative does not include LMR equipment even though federal agencies spend millions of dollars annually purchasing such equipment. By including LMR equipment in OMB's category management initiative, the government could more fully leverage its aggregate buying power to obtain the most advantageous terms and conditions for LMR procurements. OMB officials agreed that a category management approach to LMR procurement might save the government money while supporting the goal of

enhanced interoperability among agencies that require it, but OMB has not examined the feasibility of applying this approach to the procurement of LMR equipment.

Climate Change: Improved Federal Coordination Could Facilitate Use of Forward-Looking Climate Information in Design Standards, Building Codes, and Certifications

Number: GAO-17-3
Date: 11/30/2016
Summary: The houses we live in, buildings we work in, and roads and bridges we use daily are supposed to be built to last—whatever the local forecast is. The current challenge the Nation faces is that design standards and building codes generally use historical climate observations. Selected standards-developing organizations generally have not used forward-looking climate information—such as projected rainfall rates—in design standards, building codes, and voluntary certifications and instead have relied on historical observations. Further, some organizations periodically update climate information in standards, codes, and certifications, but others do not. Some standards-developing organizations have taken preliminary steps that may lead to the use of forward-looking climate information. For example, in 2015, the American Society of Civil Engineers issued a paper that recommended engineers work with scientists to better understand future climate extremes.

Standards-developing organizations face institutional and technical challenges to using the best available forward-looking climate information in design standards, building codes, and voluntary certifications, according to reports, representatives of these organizations, and federal officials. Institutional challenges include a standards-developing process that must balance various interests and can be slow to change. For example, representatives of some standards-developing organizations told GAO that their members have not expressed interest in standards that use forward-looking climate information. Technical challenges include difficulties in identifying the best available forward-looking climate information and incorporating it into standards, codes, and certifications. For example, representatives from one organization said that climate models provide a wide range of possible temperatures that is difficult to use in their standards.

Agencies have initiated some actions and could take more to help standards-developing organizations address challenges, according to various reports, representatives of standards-developing organizations, and agency officials.

Flood Insurance: FEMA Needs to Address Data Quality and Consider Company Characteristics When Revising Its Compensation Methodology

Number: GAO-17-36
Date: 12/8/2016
Summary: FEMA has yet to revise its compensation practices for Write-Your-Own (WYO) companies to reflect actual expenses as required by the Biggert-Waters Flood Insurance Reform Act of 2012 (Biggert-Waters Act), and as GAO recommended in 2009. FEMA continues to rely on insurance industry expense information for other lines of property insurance to set compensation rates for WYO companies. Efforts by FEMA, the National Association of Insurance Commissioners (NAIC)—which collects data by line of insurance from insurance companies—and

the WYO companies have resulted in some improvements to financial data on National Flood Insurance Program (NFIP) expenses that WYO companies report to NAIC. But GAO found inconsistencies among how 10 selected WYO companies (which received about 60 percent of the compensation FEMA paid in 2008–2014) reported federal flood data to NAIC that limit the usefulness of these data for determining expenses and setting compensation rates. For example, GAO analysis showed that adjusting for inconsistencies due to unreported expenses significantly reduced WYO company profits. Consequently, without quality data on actual expenses, FEMA continues to lack the information it needs to incorporate actual flood expense data into its compensation methodology as well as determine how much profit WYO companies make and whether its compensation payments are appropriate. FEMA has not clarified what other analyses it will undertake to address GAO 2009 recommendations concerning data quality. GAO also found the ways in which WYO companies operate, including how companies compensate agents and third-party vendors (with which some companies contract to conduct some or all of the management of their NFIP policies) can affect a company's expenses and profits. Considering company characteristics would allow FEMA to more effectively develop its compensation methodology and determine the appropriate amounts to reimburse WYO companies as required by the Biggert-Waters Act.

According to WYO companies and stakeholders, the current WYO arrangement and three potential alternatives GAO identified all involve trade-offs. Private insurers become WYO companies by signing a Financial Assistance/Subsidy Arrangement with FEMA and FEMA annually publishes terms for participation in the WYO program, including amounts companies will be paid for expenses. The current arrangement includes benefits for consumers from competition among approximately 75 WYO companies, but poses oversight challenges for FEMA due to the large number of companies. The three potential alternatives involve FEMA contracting with (1) one or more insurance companies to sell and service flood policies; (2) one vendor that would sell policies through agents and insurance companies would not be involved; or (3) multiple vendors to service policies while maintaining the WYO network to market and sell flood policies. All three potential alternatives would involve FEMA contracting with either WYO companies or vendors as federal contractors, a status that most WYO company representatives cited as creating more regulatory burden because of federal contract requirements. Representatives of most WYO companies and several stakeholders GAO interviewed preferred the current arrangement because of its predictability and noted that this characteristic would continue to encourage WYO company participation.

Federal Disaster Assistance: FEMA's Progress in Aiding Individuals with Disabilities Could Be Further Enhanced

Number: GAO-17-200
Date: 2/7/2017
Summary: In 2005, individuals with disabilities, individuals with limited English proficiency, and families with children were disproportionately affected by Hurricane Katrina. In response to this The Post-Katrina Act required FEMA and other entities to take certain actions to assist these individuals, such as through the establishment of a Disability Coordinator within FEMA. FEMA has taken steps to improve its disaster services for people with disabilities and its support to other entities, such as state and local governments. FEMA established the Office of Disability Integration and Coordination (ODIC) to lead the agency's efforts to promote inclusiveness in disaster planning,

response, and recovery. However, there is no established procedure for FEMA Regional Administrators, who oversee disability integration staff in the regions, to involve ODIC in the activities of these staff. As a result, regions vary in the extent to which they consult with ODIC, which has led to a lack of clarity in regional disability integration staff roles, a lack of awareness of potentially underperforming staff, and inconsistent communication between the regions and headquarters. Federal internal control standards state that organizational structures should allow the organization's components to communicate information necessary to fulfill their respective responsibilities. Communication gaps between ODIC and the regions may prevent regional disability integration staff from effectively supporting state and local governments in meeting the needs of individuals with disabilities affected by disasters. ODIC also has not established goals for how many state and local emergency managers should take its key training on integrating the needs of individuals with disabilities into disaster planning. Nor has ODIC evaluated alternative methods to deliver the training more broadly, such as virtually in addition to classroom training. As a result, state and local emergency managers may be ill-prepared to provide effective disaster services to those with disabilities.

FEMA and other entities assist individuals with limited English proficiency by translating information on disaster assistance programs. FEMA provides information about its assistance programs using print materials in other languages, bilingual staff, and a helpline with translators for more than 50 languages. State, local, and voluntary organizations also disseminate information on health and safety information, such as evacuations and sheltering: In five of the six disasters GAO reviewed where translation was needed, these entities reported using a range of services, from bilingual staff to multilingual helplines.

FEMA worked with the National Center for Missing and Exploited Children (NCMEC) to establish a national call center designed to field calls with information about children separated from their families during disasters. NCMEC also maintains a registry that serves as a web-based repository created to collect this information. However, according to FEMA officials, no disasters since Hurricane Katrina have required national child reunification support. Nevertheless, FEMA continues to work with NCMEC on maintaining reunification resources, such as by funding the deployment of NCMEC personnel following disasters.

Defense Civil Support: DOD, HHS, and DHS Should Use Existing Coordination Mechanisms to Improve Their Pandemic Preparedness

Number: GAO-17-150
Date: 2/10/2017
Summary: The Department of Defense (DOD) has developed guidance and plans to direct its efforts to provide assistance in support of civil authorities—in particular the Departments of Health and Human Services (HHS) and Homeland Security (DHS)—in the event of a domestic outbreak of a pandemic disease. For example, the Department of Defense Global Campaign Plan for Pandemic Influenza and Infectious Diseases 3551-13 provides guidance to DOD and the military services on planning and preparing for a pandemic outbreak. DOD's Strategy for Homeland Defense and Support to Civil Authorities states that DOD often is expected to play a prominent supporting role to primary federal agencies. DOD also assists those agencies in the preparedness, detection, and response to other non-pandemic viruses, such as the recent outbreak of the Zika virus.

HHS and DHS have plans to guide their response to a pandemic, but their plans do not explain how they would respond in a resource-constrained environment in which capabilities like those provided by DOD are limited. DOD coordinates with the agencies, but existing coordination mechanisms among HHS, DHS, and DOD could be used to improve preparedness. HHS's Pandemic Influenza Plan is the departmental blueprint for its preparedness and response to an influenza pandemic. DHS's National Response Framework is a national guide on how federal, state, and local governments are to respond to such incidents. DOD, HHS, and DHS have mechanisms—such as interagency working groups, liaison officers, and training exercises—to coordinate their response to a pandemic. For example, training exercises are critical in preparing these agencies to respond to an incident by providing opportunities to test plans, improve proficiency, and assess capabilities and readiness. These existing mechanisms provide the agencies opportunities to improve their preparedness and response to a pandemic. HHS and DHS plans do not specifically identify what resources would be needed to support a response to a pandemic in which demands exceeded federal resources. These officials stated that there would be no way of knowing in advance what resources would be required. HHS and DHS are in the process of updating their plans and thus have an opportunity to coordinate with each other and with DOD to determine the appropriate actions to take should DOD's support be limited.

GAO recommends that DOD, HHS, and DHS use existing coordination mechanisms to explore opportunities to improve preparedness and response to a pandemic if DOD's capabilities are limited.

Flood Insurance: Comprehensive Reform Could Improve Solvency and Enhance Resilience

Number: GAO-17-425
Date: 4/27/2017
Summary: Congress created NFIP to reduce the escalating costs of federal disaster assistance for flood damage, but also prioritized keeping flood insurance affordable, which transferred the financial burden of flood risk from property owners to the Federal Government. In many cases, premium rates have not reflected the full risk of loss, so NFIP has not had sufficient funds to pay claims. As of March 2017, NFIP owed $24.6 billion to Treasury. NFIP's current authorization expires in September 2017.

Based on discussions with stakeholders and GAO's past work, reducing federal exposure and improving resilience to flooding will require comprehensive reform of the National Flood Insurance Program (NFIP) that will need to include potential actions in six key areas (see figure below). Comprehensive reform will be essential to help balance competing programmatic goals, such as keeping flood insurance affordable while keeping the program fiscally solvent. Taking actions in isolation may create challenges for some property owners (for example, by reducing the affordability of NFIP policies) and therefore these consequences also will need to be considered. Some of the potential reform options also could be challenging to start or complete, and could face resistance, because they could create new costs for the federal government, the private sector, or property owners. Nevertheless, GAO's work suggests that taking actions on multiple fronts represents the best opportunity to help address the spectrum of challenges confronting NFIP.

To improve NFIP solvency and enhance national resilience to floods, Congress should consider comprehensive reform covering six areas: (1) outstanding debt, (2) premium rates, (3) affordability,

(4) consumer participation, (5) barriers to private-sector involvement, and (6) NFIP flood resilience efforts.

DHS OIG Reports

FEMA Needs to Improve Management of its Flood Mapping

Number: OIG-17-110
Date: 9/27/2017
Summary: Flood hazard identification and mapping is an integral part of the National Flood Insurance Program (NFIP) as it creates the foundation for floodplain management, flood insurance, and mitigation. The DHS OIG sought to determine whether the Federal Emergency Management Agency's (FEMA) Risk Mapping, Assessment and Planning Program (Risk MAP) resulted in the production of timely and accurate flood maps in accordance with NFIP requirements.

FEMA is unable to assess flood hazard miles to meet its program goal and is not ensuring mapping partner quality reviews are completed in accordance with applicable guidance. FEMA needs to improve its management and oversight of flood mapping projects to achieve or reassess its program goals and ensure the production of accurate and timely flood maps. Specifically, FEMA –

- needs to improve its financial management of flood map projects to achieve or to reassess its program goal of 80 percent New, Valid, or Updated Engineering program miles;
- has not updated its Risk MAP life cycle cost estimate to inform critical decision making;
- lacks uniform, centralized policies and procedures for projects placed on hold; and
- is not performing adequate oversight to ensure mapping partner quality reviews comply with requirements set forth in applicable guidance.

Without accurate floodplain identification and mapping processes, management, and oversight, FEMA cannot provide members of the public with a reliable rendering of their true flood vulnerability or ensure that NFIP rates reflect the real risk of flooding.

Verification Review: FEMA's Lack of Process for Tracking Public Assistance Insurance Requirements Places Billions of Tax Dollars at Risk

Number: OIG-17-50-VR
Date: 6/9/2017
Summary: A prior OIG report, which relied on the results of disaster-related audits issued by the Office of Inspector General during fiscal years 2009 to 2011, noted numerous situations where subgrantees received federal financial assistance and insurance proceeds for the same damages or where damages paid with Federal financial aid would have been covered by insurance. We also noted several instances where the final insurance settlement had not been reconciled against the funded project costs, and we identified situations in which the applicant either did not obtain adequate insurance or did not file an insurance claim.

Every year, we summarize our disaster-related audit activity in a "capping" report. Our capping reports for the 4 years following the release of our prior report (fiscal years 2012 to 2015) have

consistently identified issues relating to insurance as recurring reportable problems. In other words, we continue to see the same problems every year that we highlighted in our prior report. Under the authority of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, FEMA provides public assistance (PA) grants to states and communities to recover from presidentially declared disasters. Federal legislation and regulations require that an applicant seeking a PA grant to repair damage obtain and maintain insurance (insurance requirement) to cover losses in any future disasters. The amount of insurance coverage should be on a par with the eligible damage incurred as a result of the original disaster.3

Applicants who fail to satisfy the insurance requirement are not eligible to receive PA in ensuing disasters. However, FEMA will not require greater types and amounts of insurance than are certified as reasonably available, adequate, or necessary by the appropriate state insurance commissioner. The state insurance commissioner cannot waive Federal insurance requirements, but may certify the types and extent of insurance reasonable to protect against future loss to an insurable facility.

During the project approval process, FEMA conducts insurance reviews to ensure that applicants who received financial aid for damages in a prior disaster have satisfied the insurance requirement. FEMA will use the applicant's insurance adjustment, if known, to reduce the eligible amount of funding by the amount of the actual insurance proceeds provided. However, if this amount is unknown, a FEMA insurance specialist will review the insurance policy and damaged facility to determine the anticipated insurance proceeds and deduct this estimate from the original eligible amount.

To research historical assistance information, it is often necessary for insurance specialists to query databases that span several decades. FEMA's current system of record is EMMIE, which replaced NEMIS in 2007. NEMIS replaced the Automated Disaster Assistance Management System (ADAMS) in 1996. The Electronic Data Warehouse can generate reports based on data from NEMIS and EMMIE. However, as we noted in our prior report, data reliability and functionality issues with the contributing databases significantly limit the usefulness of EDW results.

FEMA Needs to Improve Its Oversight of the Sheltering and Temporary Essential Power Pilot Program

Number: OIG-17-38-D
Date: 2/10/2017
Summary: Following Hurricane Sandy, the New York City, Department of Environmental Protection (New York City) received $537.94 million in FEMA Public Assistance grant funds for temporary power, heat, and hot water so residents could shelter-in-place. In January 2013, FEMA estimated New York City would spend $14.33 million of this essential assistance on repairs to multifamily structures, including properties with commercial owners or operators.

Although more than 3 years have passed since the completion of the work, FEMA has not identified and recovered Federal funds New York City spent on repairs to commercial residential properties. These repairs included short-term measures such as temporary boilers and power generators. This occurred because FEMA's records were incomplete and the New York State Division of Homeland Security and Emergency Services (New York State) has not provided FEMA with a final

accounting of costs for the work. Furthermore, FEMA has no procedures to independently identify commercial residential properties New York City had assisted with Federal funds.
FEMA recognizes that commercial landlords may have received an incidental benefit from the Federal assistance provided to New York City and used for repairs to multifamily dwellings to ensure tenants could shelter in their homes. However, it is the responsibility of New York State (the grantee) to ensure that the money that FEMA provides is spent in accordance with Federal laws and regulations. Under FEMA rules, for-profit organizations are ineligible for Public

Summary and Key Findings of Fiscal Year 2015 FEMA Disaster Grant and Program Audits

Number: OIG-17-13-D
Date: 11/29/2016
Summary: This report is an annual summary, a consolidation of all of the OIG's findings and recommendations, and informs FEMA headquarters officials about significant issues of noncompliance and program inefficiencies that warrant their attention. The report also emphasizes the total resulting potential monetary benefits of the OIG's recommendations.

In fiscal year 2015, the OIG issued reports on 63 audits of FEMA grants, programs, and operations funded from the Disaster Relief Fund involving 55 grant audits and 8 program audits. During FYs 2014 and 2015, the OIG used a more proactive approach to auditing produced a significant shift from recommendations that question costs already spent to recommendations that put funds to better use before problems occur. The recommendations, if implemented, contain over $1.7 billion in potential monetary benefits, including potential cost savings in future disasters.
One troubling finding is that, of the $1.55 billion in disaster relief funds we audited, we found $457 million in questionable costs, such as duplicate payments, unsupported costs, improper contract costs, and unauthorized expenditures. This represents a 29 percent questioned-cost rate, which indicates FEMA's continued failure to manage disaster relief funds adequately. Given that the disaster relief fund averages more than $10 billion per year and FEMA grants comprise a large portion of that amount, the total amount of improper payments related to grants and other expenditures would likely reach $3 billion per year.

While FEMA has been responsive to OIG recommendations for administrative actions and for putting unspent funds to better use, it has not sufficiently held grant recipients financially accountable for improperly spending disaster relief funds. For example, it was recommended that FEMA disallow $457 million of ineligible or unsupported grant funds. However, recommendations representing 90 percent ($413 million) of those funds remain open. Further, in FYs 2009–2014, FEMA allowed 91 percent of the contract costs we recommended for disallowance for noncompliance with Federal procurement regulations, such as those that require opportunities for disadvantaged firms (e.g., small, minorities, and women) to bid on federally funded work.

Audit Tips for Managing Disaster-Related Project Costs

Number: OIG-17-120-D
Date: 9/29/2017
Summary: The Department of Homeland Security (DHS) Office of Inspector General (OIG) prepared this report to provide recipients and subrecipients (grantees and subgrantees) of Federal

Emergency Management Agency (FEMA) Public Assistance and Hazard Mitigation grant funds examples of previous audit findings. The purpose of this report was not to audit FEMA or its grant recipients and subrecipients. Rather, this report provides an overview of OIG responsibilities; roles of FEMA, recipients, and subrecipients; applicable disaster assistance Federal statutes, regulations, and guidelines; the audit process and frequent audit findings; and tips for managing project costs. Using this report should assist disaster assistance recipients and subrecipients to:

- 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.

Table of Smaller Reports

Date	Number	Title
11/8/2016	OIG-17-07-D	FEMA Should Recover $2.4 Million in Investment Gains Pennsylvania Improperly Earned on Federal Disaster Funds
1/4/2017	OIG-17-17-D	Omaha Public Power District in Nebraska Generally Accounted for and Expended FEMA Grant Funds Properly
1/5/2017	OIG-17-06-D	FEMA Should Recover $1.8 Million of $5.5 Million in Public Assistance Grant Funds Awarded to Columbia County, Florida, for Tropical Storm Debby Damages
1/9/2017	OIG-17-18-D	FEMA Should Disallow $2.0 Million of $3.59 Million Awarded to Stratford, Connecticut
1/10/2017	OIG-17-20-D	FEMA Should Disallow $577,959 of $2.9 Million Awarded to Puerto Rico Aqueduct and Sewer Authority for Hurricane Irene Damages
1/10/2017	OIG-17-19-D	Western Farmers Electric Cooperative, Oklahoma, Has Adequate Policies, Procedures, and Business Practices to Manage its FEMA Grant
1/12/2017	OIG-17-21-D	Perth Amboy, New Jersey, Effectively Managed FEMA Grant Funds Awarded for Hurricane Sandy Damages
1/23/2017	OIG-17-27-MA	Management Advisory Report: Review of FEMA Region IV Strategic Source IDIQ Contract for Office Supplies (OIG-17-27-MA)
1/24/2017	OIG-17-25-D	The Victor Valley Wastewater Reclamation Authority in Victorville, California, Did Not Properly Manage $32 Million in FEMA Grant Funds
2/1/2017	OIG-17-34-D	Columbia County Roads Department, Oregon, Needs Continued State and FEMA Assistance in Managing Its FEMA Grant
2/6/2017	OIG-17-35-D	Escambia County, Florida, Has Adequate Policies, Procedures, and Business Practices to Effectively Manage FEMA Grant Funds Awarded to Replace Its Central Booking and Detention Center
3/1/2017	OIG-17-41-D	Aiken County, South Carolina, Effectively Managed FEMA Grant Funds Awarded for Severe 2014 Winter Storm
3/20/2017	OIG-17-48-D	Iron County Forestry and Parks Department, Wisconsin, Needs Assistance and Monitoring to Ensure Proper Management of Its FEMA Grant
5/4/2017	OIG-17-57-D	Colorado County, Texas, Has Adequate Policies, Procedures, and Business Practices to Manage Its FEMA Grant

Date	Number	Title
5/24/2017	OIG-17-62-D	Texas Should Continue to Provide Deweyville Independent School District Assistance in Managing FEMA Grant Funds
6/6/2017	OIG-17-66-D	Milwaukie, Oregon, Has Adequate Policies, Procedures, and Business Practices to Manage Its FEMA Grant Funding
6/22/2017	OIG-17-77-D	FEMA Should Recover $1.5 Million in Grant Funds Awarded to Hays County, Texas
6/28/2017	OIG-17-83-D	Fort Bend County, Texas, Needs Additional Assistance and Monitoring to Ensure Proper Management of Its FEMA Grant
7/5/2017	OIG-17-93-D	FEMA Should Recover $3.9 Million of $13.2 in Grant Funds Awarded to the Borough of Lavallette, New Jersey
7/6/2017	OIG-17-95-D	Williamsburg Regional Hospital, South Carolina, Generally Accounted for and Expended FEMA Grant Funds Awarded for Emergency Work Properly
7/24/2017	OIG-17-97-D	FEMA Should Disallow $2.04 Billion Approved for New Orleans Infrastructure Repairs
8/16/2017	OIG-17-102-D	Audit of FEMA Public Assistance Grant Funds Awarded to the City of Pensacola, Florida
9/19/2017	OIG-17-106-D	Audit of FEMA Public Assistance Grant Funds Awarded to Downe Township, New Jersey
9/19/2017	OIG-17-105-D	St. Johns County, Florida, Could Benefit from Additional Technical Assistance and Monitoring to Ensure St. Johns County, Florida, Could Benefit from Additional Technical Assistance and Monitoring to Ensure Compliance with FEMA Grant Requirements
9/20/2017	OIG-17-108-D	FEMA Should Strengthen Its Policies and Guidelines for Determining Public Assistance Eligibility of PNP Schools
9/29/2017	OIG-17-118-D	FEMA Should Disallow $246,294 of $3.0 Million in Public Assistance Grant Funds Awarded to Lincoln County, Missouri
9/29/2017	OIG-17-117-D	Audit of FEMA Grant Funds Awarded to the Roman Catholic Diocese of Brooklyn, New York
9/29/2017	OIG-17-113-D	The Covington County Commission Needs Additional Assistance in Managing a $5.4 Million FEMA Grant

Federal Law Enforcement Training Center (FLETC)

GAO Reports

No GAO reports were available that aligned to this Component.

DHS OIG Reports

No DHS OIG reports were available that aligned to this Component.

Immigration and Customs Enforcement (ICE)

GAO Reports

No GAO reports were available that aligned to this Component.

DHS OIG Reports

ICE Deportation Operations

Number: OIG-17-51
Date: 4/13/2017
Summary: According to OIG, ICE does not effectively manage the deportation of aliens who are no longer detained, but are under its supervision. Effective management requires preparing and deploying the right number of employees to achieve program and policy objectives. OIG found that although many ICE Deportation Officers supervising aliens reported overwhelming caseloads and difficulty fulfilling their responsibilities, ICE does not collect and analyze data about employee workloads to allocate staff judiciously and determine achievable caseloads. Additionally, effective management also requires providing well-defined policies and procedures to employees. OIG found that ICE has not clearly and widely communicated Department of Homeland Security deportation priorities to Deportation Officers; not issued up-to-date, comprehensive, and accessible procedures; and not provided sufficient training.

ICE's failure to effectively balance and adequately prepare its workforce also makes it harder to address other obstacles to deportation, which may require significant time and resources. These management deficiencies and unresolved obstacles make it difficult for ICE to deport aliens expeditiously. ICE is almost certainly not deporting all the aliens who could be deported and will likely not be able to keep up with growing numbers of deportable aliens.

DHS Tracking of Visa Overstays is Hindered by Insufficient Technology

Number: OIG-17-56
Date: 5/1/2017
Summary: OIG found that ICE's information technology (IT) systems did not effectively support ICE's visa tracking operations. ICE personnel responsible for investigating in-country visa overstays pieced together information from dozens of systems and databases, some of which were not integrated and did not electronically share information. Despite previous efforts to improve information sharing, the DHS Chief Information Officer (CIO) did not provide the oversight and centralized management needed to address these issues. Additionally, ICE did not ensure that its field personnel received the training and guidance needed to properly use the systems currently available to conduct visa overstay tracking.

Further, the Department lacked a comprehensive biometric exit system at U.S. ports of departure to capture information on nonimmigrant visitors who exit the United States. Without a complete exit

system, DHS relied on third-party departure data, such as commercial carrier passenger manifests, to confirm a visitor's departure from the country. However, these commercial sources occasionally provided false departure or arrival status on visitors.

Because of these systems and management limitations, DHS could not account for all visa overstays in data it annually reported to Congress. Manual checking across multiple systems used for visa tracking contributed to backlogs in casework and delays in investigating suspects who potentially posed public safety or homeland security risks.

Results of Office of Inspector General FY 2016 Spot Inspections of U.S. Immigration and Customs Enforcement Family Detention Facilities

Number: OIG-17-65
Date: 6/2/2017
Summary: In July 2016 OIG did an unannounced spot inspections of ICE's three family detention facilities located in Leesport, Pennsylvania, Dilley, Texas, and Karnes, Texas. ICE uses the Family Residential Standards to govern all aspects of family detention, including medical care, nutrition, legal access, educational services, and grievances.

OIG found that the conditions of the three family detention facilities met ICE's 2007 Family Residential Standards and the facilities were clean, well-organized, and efficiently run. Based on OIG's observations, interviews, and document reviews, OIG concluded that, at all three facilities, ICE was satisfactorily addressing the inherent challenges of providing medical care and language services and ensuring the safety of families in detention.

OIG interviewed ICE and contractor staff at the three facilities to evaluate the level of training and awareness of appropriate procedures for handling allegations of sexual assault or abuse and child abuse, as well as complaints and grievances. The staff at all three facilities reported that they had received training, and all staff interviewed could identify the appropriate steps to take if they received such allegations, complaints, or grievances.

OIG also observed surveillance cameras and perimeter security at the three facilities. Staff at all three reported they store camera footage for at least 3 weeks. At one facility, staff reported that surveillance cameras cannot see certain spots in public areas. In addition, OIG observed that the facility perimeters may not prevent unauthorized intrusion.

Management Alert - Unclear Rules Regarding Executive Protection Details Raise Concerns

Number: OIG-17-103-MA
Date: 9/14/2017
Summary: As a result of whistleblower complaints, OIG examined the use of executive security and logistics details for ICE and CBP, which have created their own internal authorizations for executive protection details, staffed them, and funded them, without clear legal authority.

Except for the Secretary, the Deputy Secretary, and the Commandant of the U.S. Coast Guard, there is no statutory authority for the use of protection details and because these security details incur

substantial monetary and personnel costs, provide transportation and logistical services not necessarily tied to any demonstrated security concern, and are often authorized by those receiving the services, OIG found that these details give the appearance to some observers of being more related to executive convenience and status than protection.

OIG found that both ICE and CBP rely on the generic legacy Customs statute, 19 U.S.C. § 1589a, which permits "an officer of the customs" to "perform any other law enforcement duty that the Secretary of the Treasury may designate." The designations for both ICE and CBP rely on this statute. ICE's protection detail, known within ICE as the "Executive Logistics and Security Detail" (ELSD), was authorized by a single-page summary order issued by the Deputy ICE Director in his capacity as Acting Director in February 2014. Similarly, CBP relies on an internal, unsigned "draft" directive of its own. Both documents reference the broad legal authority delegated to each component for the performance of their functions, rather than any specific statutory authority for a security detail.

OIG noted that in contrast to ICE and CBP, other law enforcement agencies rely on express statutory language for their authorizations. Thus, agents of the Department of Justice and the Department of State are authorized specifically to provide protective services to specified senior leadership. Likewise, the statute governing the Secret Service provides a list of Executive Branch and other protectees, using straight-forward language authorizing protective activities. OIG found that neither the ICE Director nor the Commissioner of CBP is included in the Secret Service statute.

National Protection and Programs Directorate (NPPD)

GAO Reports

Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely

Number: GAO-17-163
Date: 2/1/2017
Summary: DHS's National Cybersecurity and Communications Integration Center (NCCIC) has taken steps to perform each of its 11 statutorily required cybersecurity functions, such as being a federal civilian interface for sharing cybersecurity-related information with federal and nonfederal entities. The NCCIC manages several programs that provide data used in developing 43 products and services in support of the functions. The programs include monitoring network traffic entering and exiting federal agency networks and analyzing computer network vulnerabilities and threats. The products and services are provided to its customers in the private sector; federal, state, local, tribal, and territorial government entities; and other partner organizations. For example, NCCIC issues indicator bulletins, which can contain information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents and help to fulfill its function to coordinate the sharing of such information across the government.

The National Cybersecurity Protection Act also required NCCIC to carry out its functions in accordance with nine implementing principles, to the extent practicable. However, the extent to which NCCIC adhered to the 9 principles when performing the functions is unclear because the

center has not yet determined the applicability of the principles to all 11 functions, or established metrics and methods by which to evaluate its performance against the principles. GAO identified instances where NCCIC had implemented its functions in accordance with one or more of the principles. For example, consistent with the principle that it seek and receive appropriate consideration from industry sector-specific, academic, and national laboratory expertise, NCCIC coordinated with contacts from industry, academia, and the national laboratories to develop and disseminate vulnerability alerts. On the other hand, GAO also identified instances where the cybersecurity functions were not performed in accordance with the principles. For example, NCCIC is to provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities; however, it had not established measures or other procedures for ensuring the timeliness of these assessments. Until NCCIC determines the applicability of the principles to its functions and develops metrics and methods to evaluate its performance against the principles, the center cannot ensure that it is effectively meeting its statutory requirements.

In addition, GAO identified factors that impede NCCIC's ability to more efficiently perform several of its cybersecurity functions. For example, NCCIC officials were unable to completely track and consolidate cyber incidents reported to the center, thereby inhibiting its ability to coordinate the sharing of information across the government. Similarly, NCCIC may not have ready access to the current contact information for all owners and operators of the most critical cyber-dependent infrastructure assets. This lack could impede timely communication with them in the event of a cyber incident. Until NCCIC takes steps to overcome these impediments, it may not be able to efficiently perform its cybersecurity functions and assist federal and nonfederal entities in identifying cyber-based threats, mitigating vulnerabilities, and managing cyber risks.

Federal Courthouses: Actions Needed to Enhance Capital Security Program and Improve Collaboration

Number: GAO-17-215
Date: 2/18/2017
Summary: GAO has consistently identified shortcomings in the federal government's approach to ensuring the security of federal information systems and cyber critical infrastructure as well as its approach to protecting the privacy of personally identifiable information (PII). While previous administrations and agencies have acted to improve the protections over federal and critical infrastructure information and information systems, the federal government needs to take the following actions to strengthen U.S. cybersecurity:

- Effectively implement risk-based entity-wide information security programs consistently over time. Among other things, agencies need to (1) implement sustainable processes for securely configuring operating systems, applications, workstations, servers, and network devices; (2) patch vulnerable systems and replace unsupported software; (3) develop comprehensive security test and evaluation procedures and conduct examinations on a regular and recurring basis; and (4) strengthen oversight of contractors providing IT services.
- Improve its cyber incident detection, response, and mitigation capabilities. The Department of Homeland Security needs to expand the capabilities and support wider adoption of its government-wide intrusion detection and prevention system. In addition, the federal

government needs to improve cyber incident response practices, update guidance on reporting data breaches, and develop consistent responses to breaches of PII
- Expand its cyber workforce planning and training efforts. The federal government needs to (1) enhance efforts for recruiting and retaining a qualified cybersecurity workforce and (2) improve cybersecurity workforce planning activities.
- Expand efforts to strengthen cybersecurity of the nation's critical infrastructures. The federal government needs to develop metrics to (1) assess the effectiveness of efforts promoting the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity and (2) measure and report on effectiveness of cyber risk mitigation activities and the cybersecurity posture of critical infrastructure sectors.
- Better oversee protection of personally identifiable information. The federal government needs to (1) protect the security and privacy of electronic health information, (2) ensure privacy when face recognition systems are used, and (3) protect the privacy of users' data on state-based health insurance marketplaces.

Several recommendations made by the Commission on Enhancing National Cybersecurity (Cybersecurity Commission) and the Center for Strategic & International Studies (CSIS) are generally consistent with or similar to GAO's recommendations in several areas including: establishing an international cybersecurity strategy, protecting cyber critical infrastructure, promoting use of the NIST cybersecurity framework, prioritizing cybersecurity research, and expanding cybersecurity workforces.

Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems

Number: GAO-17-518T
Date: 3/28/2017
Summary: DHS is spearheading multiple efforts to improve the cybersecurity posture of the federal government. Among these, the National Cybersecurity Protection System (NCPS) provides a capability to detect and prevent potentially malicious network traffic from entering agencies' networks. In addition, DHS's continuous diagnostics and mitigation (CDM) program provides tools to agencies to identify and resolve cyber vulnerabilities on an ongoing basis.

In January 2016, GAO reported that NCPS was limited in its capabilities to detect or prevent cyber intrusions, analyze network data for trends, and share information with agencies on cyber threats and incidents. For example, it did not monitor or evaluate certain types of network traffic and therefore would not have detected malicious traffic embedded in such traffic. NCPS also did not examine traffic for certain common vulnerabilities and exposures that cyber threat adversaries could have attempted to exploit during intrusion attempts. In addition, at the time of the review, federal agencies had adopted NCPS to varying degrees. GAO noted that expanding NCPS's capabilities, such as those for detecting and preventing malicious traffic and developing network routing guidance, could increase assurance of the system's effectiveness in detecting and preventing computer intrusions and support wider adoption by agencies. By taking these steps, DHS would be better positioned to achieve the full benefits of NCPS.

The tools and services delivered through DHS's CDM program are intended to provide agencies with the capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels. In May 2016, GAO reported that most of the 17 civilian agencies covered by the Chief Financial Officers Act that also reported having high-impact systems were in the early stages of CDM implementation. For example, 14 of the 17 agencies reported that they had deployed products to automate hardware and software asset inventories, configuration settings, and common vulnerability management but only 2 had completed installation of agency and bureau/component-level dashboards. Some of the agencies noted that expediting CDM implementation could be of benefit to them in further protecting their high-impact systems. GAO concluded that the effective implementation of the CDM program can assist agencies in resolving cybersecurity vulnerabilities that expose their information systems and information to evolving and pernicious threats. By continuing to make available CDM tools and capabilities to agencies, DHS can have additional assurance that agencies are better positioned to protect their information system and information.

In addition, DHS offered other services such as monthly operational bulletins, CyberStat reviews, and cyber exercises to help protect federal systems. In May 2016, GAO reported that although participation varied among the agencies surveyed, most agencies had found that the services were very or somewhat useful. By continuing to make these services available to agencies, DHS is better able to assist agencies in strengthening the security of their information systems.

Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges

Number: GAO-17-533T
Date: 4/4/2017
Summary: GAO and others have identified a number of key challenges facing federal agencies in ensuring that they have an effective cybersecurity workforce:

- Identifying skills gaps: As GAO reported in 2011, 2015, and 2016, federal agencies have faced challenges in effectively implementing workforce planning processes for information technology (IT) and defining cybersecurity staffing needs. GAO also reported that the Office of Personnel Management (OPM) could improve its efforts to close government-wide skills gaps.
- Recruiting and retaining qualified staff: Federal agencies continue to be challenged in recruiting and retaining qualified cybersecurity staff. For example, in August 2016, GAO reported that federal chief information security officers faced significant challenges in recruiting and retaining personnel with high-demand skills.
- Federal hiring activities: The federal hiring process may cause agencies to lose out on qualified candidates. In August 2016 GAO reported that OPM and agencies needed to assess available federal hiring authorities to more effectively meet their workforce needs.

To address these and other challenges, several executive branch initiatives have been launched and federal laws enacted. For example, in July 2016, OPM and the Office of Management and Budget issued a strategy with goals, actions, and timelines for improving the cybersecurity workforce. In addition, laws such as the Federal Cybersecurity Workforce Assessment Act of 2015 require agencies to identify IT and cyber-related positions of greatest need.

Further, other ongoing activities have the potential to assist agencies in developing, recruiting, and retaining an effective cybersecurity workforce. For example:

- Promoting cyber and science, technology, engineering, and mathematics (STEM) education: A center funded by DHS developed a kindergarten to 12th grade-level cyber-based curriculum that provides opportunities for students to become aware of cyber issues, engage in cyber education, and enter cyber career fields.
- Cybersecurity scholarships: Programs such as Scholarship for Service provide tuition assistance to undergraduate and graduate students studying cybersecurity in exchange for a commitment to federal service.
- National Initiative for Cybersecurity Careers and Studies: DHS, in partnership with several other agencies, launched the National Initiative for Cybersecurity Careers and Studies in 2013 as an online resource to connect government employees, students, educators, and industry with cybersecurity training providers across the nation.

If effectively implemented, these initiatives, laws, and activities could further agencies' efforts to establish the cybersecurity workforce needed to secure and protect federal IT systems.

Technology Assessment: Internet of Things: Status and implications of an increasingly connected world

Number: GAO-17-75
Date: 5/15/2017
Summary: The Internet of Things (IoT) refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information. These "smart" devices are increasingly being used to communicate and process quantities and types of information that have never been captured before and respond automatically to improve industrial processes, public services, and the well-being of individual consumers. For example, a "connected" fitness tracker can monitor a user's vital statistics, and store the information on a smartphone. A "smart" tractor can use GPS-based driving guidance to maximize crop planting or harvesting.

Electronic processors and sensors have become smaller and less costly, which makes it easier to equip devices with IoT capabilities. This is fueling the global proliferation of connected devices, allowing new technologies to be embedded in millions of everyday products. The IoT's rapid emergence brings the promise of important new benefits, but also presents potential challenges such as the following:
• Information security. The IoT brings the risks inherent in potentially unsecured information technology systems into homes, factories, and communities. IoT devices, networks, or the cloud servers where they store data can be compromised in a cyberattack. For example, in 2016, hundreds of thousands of weakly-secured IoT devices were accessed and hacked, disrupting traffic on the Internet.

- Privacy. Smart devices that monitor public spaces may collect information about individuals without their knowledge or consent. For example, fitness trackers link the data they collect to online user accounts, which generally include personally identifiable

information, such as names, email addresses, and dates of birth. Such information could be used in ways that the consumer did not anticipate. For example, that data could be sold to companies to target consumers with advertising or to determine insurance rates.

- Safety. Researchers have demonstrated that IoT devices such as connected automobiles and medical devices can be hacked, potentially endangering the health and safety of their owners. For example, in 2015, hackers gained remote access to a car through its connected entertainment system and were able to cut the brakes and disable the transmission.
- Standards. IoT devices and systems must be able to communicate easily. Technical standards to enable this communication will need to be developed and implemented effectively.
- Economic issues. While impacts such as positive growth for industries that can use the IoT to reduce costs and provide better services to customers are likely, economic disruptions are also possible, such as reducing the need for certain types of businesses and jobs that rely on individual interventions, including assembly line work or commercial vehicle deliveries.

Critical Infrastructure Protection: DHS Has Fully Implemented Its Chemical Security Expedited Approval Program, and Participation to Date Has Been Limited

Number: GAO-17-502
Date: 6/29/2017
Summary: DHS fully implemented the Chemical Facility Anti-Terrorism Standards (CFATS) Expedited Approval Program in June 2015 and reported to Congress on the program in August 2016, as required by the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (CFATS Act of 2014). DHS's expedited program guidance identifies specific security measures that eligible (i.e., tiers 3 and 4) high-risk facilities can use to develop expedited security plans, rather than developing standard (non-expedited) security plans. Standard plans provide more flexibility in securing a facility, but are also more time-consuming to process. DHS's report to Congress on the expedited program discussed all required elements. For example, DHS was required to assess the impact of the expedited program on facility security. DHS reported that it was difficult to assess the impact of the program on security because only one facility had used it at the time of the report. DHS officials stated that they would further evaluate the impact of the program on security if enough additional facilities use it in the future.

As of April 2017, only 2 of the 2,496 eligible facilities opted to use the Expedited Approval Program; various factors affected participation. Officials from the two facilities told GAO they used the program because its prescriptive nature helped them quickly determine what they needed to do to implement required security measures and reduced the time and cost to prepare and submit their security plans to DHS. According to DHS and industry officials GAO interviewed, low participation to date could be due to several factors:

- DHS implemented the expedited program after most eligible facilities already submitted standard (non-expedited) security plans to DHS;
- the expedited program's security measures may be too strict and prescriptive, not providing facilities the flexibility of the standard process; and
- DHS conducts in-person authorization inspections to confirm that security plans address risks under the standard process, but does not conduct them under the expedited program.

DHS officials noted that some facilities may prefer having this inspection because it provides them useful information.

Recent changes in the CFATS program could also affect future use of the expedited program. In fall 2016, DHS updated its online tool for gathering data from facilities. Officials at DHS and 5 of the 11 industry organizations GAO contacted stated that the revised tool is more user-friendly and less burdensome than the previous one; however, it is unclear how the new tool might affect future use of the expedited program.

DHS OIG Reports

No DHS OIG reports were available that aligned to this Component.

Science and Technology (S&T)

GAO Reports

Bioforensics: DHS Needs to Conduct a Formal Capability Gap Analysis to Better Identify and Address Gaps

Number: GAO-17-177
Date: 1/11/2017
Summary: DHS and the Federal Bureau of Investigation (FBI) have identified some gaps in their bioforensics capabilities, but DHS has not performed a formal bioforensics capability gap analysis. It is therefore not clear whether DHS and the FBI have identified all of their capability gaps. A capability gap analysis can help identify deficiencies in capabilities and can help support the validation and prioritization of how to address the gaps. DHS and the FBI have identified capability gaps using an informal undocumented process. For example, DHS held informal meetings to seek FBI input on capability gaps associated with recent casework. Gaps identified through this informal process include the inability to (1) characterize unique, novel, and engineered agents and "unknowns" (emerging or synthetic organisms) and (2) understand and communicate uncertainty associated with analyzing complex biological samples, among other things. In the absence of a well-documented bioforensics capability gap analysis, the rationale for DHS's resource allocations, or its plans for future enhancements to existing capabilities are not clear and thus cannot ensure that resources are being targeted to the highest priority gaps.

In addition to DHS and the FBI, other organizations, such as the National Research Council (NRC) of the National Academy of Sciences (NAS), and the National Science and Technology Council (NSTC) of the Office of Science and Technology Policy (OSTP), have identified potential bioforensics capability needs. These needs can generally be grouped into three areas: science, technology and methods, and bioinformatics and data. GAO also convened a meeting of experts, with the help of NAS, and these experts updated a list of potential bioforensics capability needs that NAS and OSTP had previously identified within each of these areas. Some of the needs these experts confirmed as still relevant were similar to those DHS and FBI officials have identified, while others were different. For example, like DHS and the FBI, the experts agreed that an ability

to characterize genetically engineered agents was needed, but they also suggested that evaluating existing protocols, such as those for DNA sequencing, to determine whether they were validated, was needed. GAO believes that this information may be helpful to DHS and the FBI as part of any future bioforensics capability gap analysis they undertake.

Since 2010, DHS has enhanced some of its bioforensics capabilities, with FBI input, by focusing on developing methods-based capabilities while maintaining agent-based capabilities. DHS has funded research and development projects addressing areas such as genome sequencing approaches, which underpin many methods-based bioforensics capabilities. DHS is also developing an in-house reference collection for use in investigations. In addition, DHS is developing the ability to characterize unique, novel agents as well as "unknowns," such as synthetic organisms. DHS projects that some enhanced capabilities will be complete in about 2025. However, in pursuing enhancements, DHS faces several challenges, including establishing a statistical framework for interpreting bioforensics analyses and associated inferences and communicating them in a court setting, as well as obtaining suitable biological agents and DNA sequences to ensure quality references for use in investigations.

DHS OIG Reports

No DHS OIG reports were available that aligned to this Component.

Transportation Security Administration (TSA)

GAO Reports

Radioactive Sources: Opportunities Exist for Federal Agencies to Strengthen Transportation Security

Number: GAO-17-58
Date: 2/7/2017
Summary: Concerns have been raised that risk-significant sources could be stolen by terrorists and used to create a "dirty bomb." The Nuclear Regulatory Commission (NRC) is responsible for licensing the possession and use of these sources. The Department of Transportation regulates the transport of such sources, and DHS is responsible for securing all modes of transportation. GAO was asked to review the security of these sources during ground transport. This report examines (1) the steps that NRC, DOT, and DHS have taken since September 11, 2001, to strengthen the security of these sources; and (2) the challenges that exist to further strengthening the security of these sources during ground transport and opportunities to address them.

Aviation Security: TSA Does Not Have Valid Evidence Supporting Most of the Revised Behavioral Indicators Used in Its Behavior Detection Activities

Number: GAO-17-608R
Date: 7/20/2017
Summary: Over the past 10 years, TSA has employed thousands of trained behavior detection officers (BDO) to identify passengers exhibiting behaviors indicative of stress, fear, or deception at airport screening checkpoints. According to TSA, certain verbal and nonverbal cues and behaviors—TSA's behavioral indicators—may indicate mal-intent, such as the intent to carry out a terrorist attack. 1 These behavioral indicators include, for example, assessing the way an individual swallows or the degree to which an individual's eyes are open. According to TSA, such indicators provide a means for identifying passengers who may pose a risk to aviation security and referring them for additional screening. 2 TSA officials have reported that behavior detection methods are based on techniques that have been used by defense organizations and law enforcement agencies for years. However, we reported in November 2013 that available evidence did not support whether behavioral indicators can be used to identify persons who may pose a risk to aviation security. 3 Specifically, we reported that TSA had not demonstrated that BDOs could consistently identify the behavioral indicators and that the subjectivity of the indicators and variation in BDO referral rates raised questions about TSA's continued use of these indicators. Further, we found that decades of peer-reviewed, published research on the complexities associated with detecting deception through human observation also called into question the scientific basis for TSA's behavior detection activities. As a result, we recommended in November 2013 that TSA limit future funding for the agency's behavior detection activities until TSA can provide scientifically validated evidence that demonstrates that behavioral indicators can be used to identify passengers who may pose a threat to aviation security.

Aviation Security: TSA Has Made Progress Implementing Requirements in the Aviation Security Act of 2016

Number: GAO-17-662
Date: 9/7/2017
Summary: Recent incidents involving aviation workers conducting criminal activity in the nation's commercial airports have led to interest in the measures TSA and airport operators use to control access to secure areas of airports. The 2016 Aviation Security Act (ASA) required TSA to take several actions related to oversight of access control security at airports. The Act also contains a provision for GAO to report on progress made by TSA.

This report examines, among other issues, progress TSA has made in addressing the applicable requirements of the 2016 ASA. GAO compared information obtained from TSA policies, reports, and interviews with TSA officials to the requirements in the 2016 ASA. GAO also visited three airports to observe their use of access controls and interviewed TSA personnel. The non-generalizable group of airports was selected to reflect different types of access control measures and airport categories.

Aviation Security: Actions Needed to Systematically Evaluate Cost and Effectiveness Across Security Countermeasures

Number: GAO-17-794
Date: 9/11/2017
Summary: TSA has data on the effectiveness of some, but not all of its passenger aviation security countermeasures. Specifically, TSA has data on passenger prescreening, checkpoint and checked baggage screening, and explosives detection canines. Further, TSA is taking steps to improve the quality of this information. However, it does not have effectiveness data for its Behavior Detection and Analysis (BDA) program and the U.S. Federal Air Marshal Service (FAMS). For BDA—a program to identify potential threats by observing passengers for behaviors indicative of stress, fear, or deception—in July 2017, GAO reported that (1) TSA does not have valid evidence supporting most of its behavioral indicators, and (2) TSA should continue to limit future funding for its behavior detection activities until it can provide such evidence. For FAMS—a program that deploys armed law enforcement officers on certain flights at an annual cost of about $800 million for fiscal year 2015—officials reported that one of the primary security contributions is to deter attacks. However, TSA does not have information on its effectiveness in doing so, nor does it have data on the deterrent effect resulting from any of its other aviation security countermeasures. While officials stated that deterrence is difficult to measure, the Government Performance and Results Act of 1993, as updated, provides that agencies are to assess the effectiveness of their programs. Further, the Office of Management and Budget and GAO have suggested approaches for measuring deterrence. Developing such methods for TSA countermeasures, especially for an effort such as FAMS in which the primary goal is deterrence, would enable TSA to determine whether its substantial investment is yielding results.

Aviation Security: TSA's Efforts to Assess Foreign Airports and Inspect Air Carriers

Number: GAO-17-808T
Date: 9/26/2017
Summary: GAO's preliminary analysis showed that TSA has taken steps to enhance its foreign airport assessments and air carrier inspections since 2011, including aligning program resources based on risk, resolving airport access issues, making evaluations more comprehensive, and creating operational efficiencies. For example, TSA has implemented targeted foreign airport assessments in appropriate locations based on risk; begun primarily assessing airports in Europe through joint assessments with the European Commission; and developed the Global Risk Analysis and Decision Support System to streamline the assessment report writing process and strengthen data analysis capabilities, among other actions. GAO's preliminary analysis also found that TSA assists foreign airports in addressing identified security deficiencies through various types of capacity development efforts, such as on-the-spot counseling and consultation, and training and technical assistance. TSA also assists air carriers in addressing identified security deficiencies through on-the-spot counseling as well as providing clarification regarding TSA security requirements when necessary. While TSA has taken steps to strengthen its analytical processes, among other things, GAO's preliminary analysis showed that TSA lacks key information for decision making. Specifically, TSA's database for tracking the resolution status of security deficiencies does not have comprehensive data on security deficiencies' root causes and corrective actions. For example, GAO found that 70 percent

of fiscal year 2016 records in TSA's database exhibited empty fields pertaining to root cause or recommended corrective action. In addition, the database does not have a field to categorize specific root causes. For example, while it captures three broad categories of root causes—lack of knowledge, lack of infrastructure, and lack of will—it does not capture 12 subcategories (e.g., supervision) that would better explain the root causes of particular security deficiencies. By fully collecting data and improving the categorization of root causes, TSA would be better positioned to assure that corrective actions accurately address the specific, underlying reasons for security vulnerabilities.

DHS OIG Reports

TSA's Office of Intelligence and Analysis Has Improved Its Field Operations

Number: OIG-17-107
Date: 9/20/2017
Summary: Although a complainant alleged there were systemic security and operational challenges in TSA's Office of Intelligence and Analysis, (OIA), the Office of the Inspector General (OIG) identified few documented security incidents over the past 5 years, all of which OIA addressed with corrective actions. Further, OIA has improved the effectiveness of the Field Intelligence Division (FID) and the Field Intelligence Officer program by hiring qualified, experienced intelligence professionals and implementing clear policies and procedures to guide officers, but it could enhance training of Field Intelligence Officers. In addition, OIA is addressing identified weaknesses in coordination among its watches and perceived delays in intelligence reporting.

TSA Could Improve Its Oversight of Airport Controls over Access Media Badges (Redacted)

Number: OIG-17-04
Date: 10/14/2016
Summary: Based on its comprehensive and targeted inspections, TSA has asserted that most airports adequately control badges for employees working in nonpublic areas. However, from the results of special inspections conducted by TSA in 2015, as well as OIG testing, OIG concludes that airports do not always properly account for these badges after they are issued. TSA's current inspection practice of relying on information reported by airports about access media badges limits its oversight of badge controls. By testing more controls, which are designed to curtail the number of unaccounted for badges, TSA could strengthen its oversight of airports. Improved oversight by TSA, including encouraging wider use of airports' best practices, would help mitigate the risks to airport security posed by unaccounted for employee badges.

Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports (Redacted)

Number: OIG-17-14
Date: 12/30/2016
Summary: Previous OIG reports identified numerous deficiencies in security controls for TSA's IT systems and equipment at airports. These deficiencies included inadequate physical security for TSA server rooms at airports, unpatched software, missing security documentation, and incomplete reporting of IT costs. TSA has undertaken various actions to address the recommendations we made in these reports. Based on OIG's review of the corrective actions taken as of May 2016, OIG considers most of the recommendations resolved and closed. However, TSA has not yet resolved recommendations made in two key areas. TSA officials indicate it will take time, money, and contract changes to include security requirements in the Security Technology Integrated Program, a data management system that connects airport screening equipment to servers. TSA also disagrees that closed-circuit televisions, including cameras, at airports constitute IT equipment and that TSA is responsible for maintaining them.

The Federal Air Marshal Service Has Sufficient Policies and Procedures for Addressing Misconduct

Number: OIG-17-104
Date: 9/13/2017
Summary: The Federal Air Marshal Service (FAMS) is a division of TSA. FAMS is responsible for promoting confidence in civil aviation by deploying Federal air marshals to detect, deter, and defeat hostile acts targeting transportation systems. Because of its law enforcement mission, FAMS developed a series of unique policies and procedures to address conduct related to air marshals' specific duties, while also operating under the purview of TSA's conduct code and misconduct policies and procedures. FAMS has sufficient policies and procedures to establish expectations for appropriate conduct, identify misuse of Government resources, and address misconduct allegations. FAMS' policies specifically require all employees to report suspected misconduct. Additionally, TSA and FAMS have a systematic and multilayered process for handling FAMS misconduct issues, which includes review of misconduct allegations by two separate and independent offices.

U.S. Citizenship and Immigration Services (USCIS)

GAO Reports

Immigration Benefits System: Significant Risks in USCIS's Efforts to Develop its Adjudication and Case Management System

Number: GAO-17-486T
Date: 3/16/2017
Summary: Every year, USCIS processes millions of applications from foreign nationals seeking to study, work, visit, or live in the United States, and for persons seeking to become U.S. citizens. In

2006, USCIS began the Transformation Program to enable electronic adjudication and case management tools that would allow users to apply and track their applications online.

USCIS's most recent cost and schedule baseline, approved in April 2015, indicates that its Transformation Program will cost up to $3.1 billion and be fully deployed no later than March 2019. This is an increase of approximately $1 billion with a delay of more than 4 years from its initial July 2011 acquisition program baseline. In addition, the program is currently working to develop a new cost and schedule baseline to reflect further delays. Due to the program's recurring schedule delays, USCIS will continue to incur costs for maintaining its existing systems while the program awaits full implementation. Moreover, USCIS's ability to achieve program goals, including enhanced national security, better customer service, and operational efficiency improvements, will be delayed.

Recurring delays are partly the result of challenges in program management. In July 2016, GAO reported that the USCIS Transformation Program had fully addressed some, and partially addressed many other key practices for implementing software development, conducting systems integration and testing, and monitoring the largest program contractors. Nevertheless, GAO reported that the program inconsistently adhered to these practices. For example:

- The program had established an environment and procedures for continuously integrating functionality and was conducting various tests and inspections of new software code. However, the program was not consistently adhering to its policies and guidance or meeting stated benchmarks for testing and inspections.
- The program had reported experiencing issues such as production defects and bugs in the system as a result of deploying software that had not been fully tested.
- The program had mixed success in monitoring its contractors for six contracts that GAO reviewed. For example, a development services contract contained appropriate performance criteria that linked to the program goals, but the program did not clearly define measures against which to analyze differences between services expected and those delivered.
- Its software development approach deviated from key practices in part because USCIS policy and guidance were not being updated.

Given the history of development for the Transformation Program and the subsequent commitment of additional resources for a new system, it is more important than ever that USCIS consistently follow key practices in its system development efforts. For example, the program has already reported realizing risks associated with deploying software that has not been fully tested, such as system bugs, defects, and unplanned network outages. If the agency does not address the issues GAO has identified in prior work, then it will continue to experience significant risk for increased costs, further schedule delays, and performance shortfalls.

Immigration Benefits System: Significant Risks in USCIS's Efforts to Develop its Adjudication and Case Management System

Number: GAO-17-486T
Date: 3/16/2017
Summary: Congress created the Employment-Based Fifth Preference (EB-5) immigrant visa category to promote job creation and encourage capital investment in the United States by foreign investors. EB-5 Immigrant Investor Program (EB-5 Program) requirements include investing $1 million in a new business that will result in the creation of at least 10 full-time positions for qualifying employees, or a reduced amount of $500,000 if the investment is made in a targeted employment area (TEA)—defined as an area that is rural or has an unemployment rate at least 150 percent of the national average. About 10,000 EB-5 visas per fiscal year are made available to qualified immigrant investors and their families seeking to immigrate to the United States through the EB-5 Program. Prospective program participants submit petitions to the Department of Homeland Security's U.S. Citizenship and Immigration Services for adjudication, along with supporting materials.

GAO estimated from its September 2016 review of a generalizable random sample of unadjudicated I-526 (Immigrant Petition by Alien Entrepreneur) petitions that about 99 percent of the 6,652 EB-5 petitioners who filed a petition in the fourth quarter of fiscal year 2015 elected to invest in a project located in a TEA. The remaining one percent of petitioners elected to invest in a project that was not located in a TEA. In September 2016, GAO also estimated that about 90 percent of petitioners from the fourth quarter of fiscal year 2015 electing to invest in a high unemployment TEA, based the TEA on the average unemployment rate for a combination of census areas, as allowed under the program. The remaining petitioners (10 percent) based the TEA on the unemployment rate of a single census tract, census block group, or county. Of the 90 percent of petitioners from the fourth quarter of fiscal year 2015 who based a high unemployment TEA on the average unemployment rate of a combination of census areas, GAO estimated that 63 percent combined 2 to 10 census areas, 26 percent combined 11 to 100 census areas, and 12 percent combined more than 100 census areas.

For petitioners from the fourth quarter of fiscal year 2015 who elected to invest in a TEA, GAO estimated in September 2016 that about 74 percent invested or planned to invest in various types of real estate projects including mixed use, hotels and resorts, commercial, and residential developments; while the remaining petitioners invested or planned to invest in projects such as infrastructure projects or transportation, restaurants, medical, and education facility projects. Further, EB-5 investment in projects located in a TEA was generally less than non-EB-5 investment by other foreign or U.S. investors. GAO estimated that the median percentage of total potential EB-5 investment was 29 percent of the total estimated project cost, and the estimated mean percentage was 40 percent.

Immigration Status Verification for Benefits: Actions Needed to Improve Effectiveness and Oversight

Number: GAO-17-204
Date: 3/23/2017
Summary: USCIS has taken steps to assess the accuracy of the information reported by its Systematic Alien Verification for Entitlements (SAVE) system. Millions of applicants for healthcare, licenses, and other benefits rely on SAVE system to verify their immigration or naturalized or derived citizenship status at the request of over 1,000 federal, state, and local user agencies. Agencies use the information from SAVE to help determine an applicant's eligibility for benefits. Programs required or authorized to participate include Medicaid, certain license-issuing programs (such as driver's licenses), federal food and housing assistance, and educational programs. This report examines the extent to which USCIS has (1) determined the accuracy of SAVE information, (2) instituted safeguards to protect privacy and provide the ability to correct erroneous information, and (3) monitored user agency compliance with SAVE program policies.

Since 2014 USCIS has conducted monthly checks to ensure SAVE is accurately reporting information contained in its source systems. In addition, USCIS reports that SAVE status verifiers, who manually research a benefit applicant's immigration status during a process known as additional verification, accurately reported the applicant's status 99 percent of the time. However, from fiscal year 2012 through fiscal year 2016, GAO found that the majority of SAVE user agencies that received a SAVE response prompting them to institute additional verification did not complete the required additional steps to verify the benefit applicant's immigration status. USCIS does not have sufficient controls to help ensure agencies are completing the necessary steps because of inconsistent guidance, and lacks reasonable assurance that SAVE user agencies have completed training that explains this procedure. Improving guidance and ensuring training on verification requirements could help USCIS better ensure agencies have complete and accurate information for making eligibility determinations.

GOA noted that USCIS has also taken actions to protect the privacy of personal information related to SAVE, such as requiring SAVE user agencies to sign a memorandum of agreement (MOA) stating the intended use of the system and provisions for safeguarding information. GAO found that USCIS established mechanisms for access, correction, and redress regarding use of an individual's personal information; however, GAO determined that these mechanisms were largely ineffective and unlikely to enable benefit applicants to make timely record corrections. Specifically, USCIS provides a fact sheet for benefit applicants stating their immigration status could not be verified, along with information on contacting DHS to update or correct their records. However, the fact sheet's guidance on contacting DHS was not specific or clear, which could hinder benefit applicants' efforts to contact DHS. Without an effective method for ensuring individuals can access and correct their information, benefit applicants may face challenges ensuring accurate information is used in a SAVE check and appealing potentially erroneous denials of benefits with the user agency in a timely manner.

According to GAO, USCIS's SAVE Monitoring and Compliance (M&C) branch who monitors user agencies' use of SAVE in accordance with their MOA found that M&C's efforts have not improved agency compliance rates for the two monitored behaviors—deleting inactive user accounts and instituting additional verification when prompted. For example, GAO found that only 4 of 40

agencies monitored from fiscal years 2013 through 2015 had improved their compliance with requirements to complete additional verification when prompted. Further M&C does not have a documented, risk-based strategy for monitoring. Without such a strategy, USCIS is not well-positioned to target its monitoring efforts on the agencies most in need of compliance assistance or ensure the most effective use of its limited resources.

Refugees: Actions Needed by State Department and DHS to Further Strengthen Applicant Screening Process and Assess Fraud Risks

Number: GAO-17-706
Date: 7/31/2017
Summary: From fiscal year 2011 through June 2016, the U.S. Refugee Admission Program (USRAP) received about 655,000 applications and referrals—with most referrals coming from the United Nations High Commissioner for Refugees—and approximately 227,000 applicants were admitted to the United States. USCIS conducts in-person interviews with applicants and assesses eligibility for refugee status to determine whether to approve or deny them for resettlement.

GAO found that although, USCIS has policies and procedures for adjudicating applications it could improve training, the process for adjudicating applicants with national security concerns, and quality assurance assessments. For example, USCIS has developed an assessment tool that officers are to use when interviewing applicants. GAO observed 29 USCIS interviews and found that officers completed all parts of the assessment. GAO found that USCIS also provides specialized training to all officers who adjudicate applications abroad, but could provide additional training for officers who work on a temporary basis, which would better prepare them to adjudicate applications.

GOA noted that USCIS has taken steps to address challenges with adjudicating cases. For example, in 2016, USCIS completed a pilot that included sending officers with national security expertise overseas to support interviewing officers in some locations. USCIS determined the pilot was successful and has taken steps to formalize it. However, USCIS has not developed and implemented a plan for deploying these additional officers, whose expertise could help improve the efficiency and effectiveness of the adjudication process. Further GOA found that, USCIS does not conduct regular quality assurance assessments of refugee adjudications, consistent with federal internal control standards. Conducting regular assessments of refugee adjudications would allow USCIS to target training or guidance to areas of most need.

DHS OIG Reports

Better Safeguards Are Needed in USCIS Green Card Issuance

Number: OIG-17-11
Date: 11/21/2016
Summary: In March 2016, OIG reported challenges in USCIS' automation of benefits processing. OIG's follow-up review concluded that USCIS continues to struggle to ensure proper Green Card issuance. OIG found that over the past 3 years, USCIS produced at least 19,000 cards that included

incorrect information or were issued in duplicate. Most card issuance errors were due to design and functionality problems in ELIS, which is being implemented to automate benefits processing. USCIS' efforts to address the errors have been inadequate. Although USCIS conducted a number of efforts to recover the inappropriately issued cards, these efforts also were not fully successful and lacked consistency and a sense of urgency. Over the last 3 years, USCIS received over 200,000 reports from approved applicants about missing cards. The number of cards sent to wrong addresses has incrementally increased since 2013 due in part to complex processes for updating addresses, ELIS limitations, and factors beyond the agency's control. Improperly issued Green Cards pose significant risks and burdens for the agency. Errors can result in approved applicants being unable to obtain benefits, maintain employment, or prove lawful immigration status. In the wrong hands, Green Cards may enable terrorists, criminals, and illegal aliens to remain in the United States and access immigrant benefits. Responding to card issuance errors has also resulted in additional workload and corresponding costs, as USCIS spent just under $1.5 million to address card related customer inquiries in fiscal year 2015.

Verification Review of USCIS' Progress in Implementing OIG Recommendations for SAVE to Accurately Determine Immigration Status of Individuals Ordered Deported

Number: OIG-17-23-VR
Date: 1/18/2017
Summary: OIG found that USCIS' progress in implementing recommendations from the, *Improvements Needed for the SAVE (Systematic Alien Verification for Entitlements Program) to Accurately Determine Immigration Status of Individuals Ordered Deported (OIG-1311, December 2012) OIG* report. The report assessed the Systematic Alien Verification for Entitlements (SAVE), a Web-based system that uses the Verification Information System (VIS) to provide almost instantaneous responses to immigrant status inquiries.

OIG reported that USCIS has addressed the 4 recommendations including implementing a Review Information Exchange System (IRIES) to have timely status of individuals who have lost status as a result of a final removal order or expiration of time permitted to file an appeal. OIG also found that USCIS develop an automated interface that would result in SAVE accurately reflecting the immigration status of individuals ordered deported. OIG also confirmed during its verification review that USCIS reasonably validated the accuracy of SAVE's initial verification process and continue to monitor initial verification results for specific populations that may be at risk of erroneous verification.

Management Alert - U.S. Citizenship and Immigration Services' Use of the Electronic Immigration System for Naturalization Benefits Processing

Number: OIG-17-26-MA
Date: 1/19/2017
Summary: In March 2016, OIG had identified a number issues with the Electronic Immigration System (ELIS) – a system for processing immigrant naturalization applications. OIG found ELIS had system functionality and performance problems as well as security concerns regarding inadequate applicant background check and frequent system outages and problems with system interfaces that negatively affected productivity. OIG reported that USCIS Field Operations

Directorate identified the following four top challenges in working in ELIS that field users believe must be addressed to ensure effective naturalization processing.

1. Deficiencies in Background and Security Checks for Applicants: USCIS personnel are required to check applicants' biographic data against U.S. Customs and Border Protection's TECS system and the Federal Bureau of Investigation's name check database. However, ELIS allows cases to be moved forward for processing despite incomplete or inaccurate background and security checks. According to Field Operations Directorate officials, approximately 175 applicants were granted citizenship as of January 11, 2017 before the problem was detected and USCIS began redoing the name checks to ensure they were all completed correctly. Without sufficient vetting, immigrants could potentially be granted U.S. citizenship although they are ineligible or pose national security threats.
2. Inconsistent Case Management Update and Closeout: ELIS does not consistently update the USCIS Central Index System with final immigrant status once an individual is naturalized. The Central Index System contains official records and decisions on all individuals who apply for benefits. The system must accurately reflect final benefits decisions in order to officially close out cases, record applicant status, and inform DHS components such as U.S. Customs and Border Patrol and U.S. Immigration and Customs Enforcement.
3. Printing problems: USCIS field officers cannot print naturalization certificates directly through ELIS, requiring time consuming workarounds to configure individual workstations to print through alternate systems. More importantly, printed certificates sometimes included incorrect names or lacked mandatory data such as photos or country of origin, rendering them invalid. Both issues have created backlogs in benefits delivery.
4. Lack of Contingency Planning for Sustained Processing: USCIS field officers are unable to obtain electronic copies of applicant files and supporting evidence during frequent ELIS or network outages.

Due to these problems, U.S. Citizenship and Immigration Services (USCIS) decided to revert to legacy processing and discontinue using ELIS to process new naturalization applications. In January 2017, OIG found that USCIS leadership decided to return to using ELIS. OIG reports that the system deficiencies with ELIS remain unresolved and is recommending that USCIS halt plans to revert to using ELIS until USCIS successfully addresses the issues.

H-2 Petition Fee Structure is Inequitable and Contributes to Processing Errors

Number: OIG-17-42
Date: 3/6/2017
Summary: USCIS' H-2 program enables employers to petition to bring temporary non-immigrant workers into the United States. OIG found that H-2 petition fee structure is inequitable and contributes to processing errors. Federal guidelines indicate that beneficiaries should pay the cost of services from which they benefit. However, OIG found that USCIS charged employers a flat fee of $325 per H-2 petition ($460 as of December 23, 2016), regardless of whether it was to bring one or hundreds of temporary nonimmigrant workers into the United States. Each worker listed on a petition must be vetted through an extensive adjudication process, for the most part within 15 days.

According to OIG, USCIS officials stated that their systems do not capture the time to adjudicate petitions with various numbers of workers, which is needed to equitably set the H-2 petition fee. As such, USCIS instituted the flat fee structure because it is easy to manage. USCIS also did not limit the number of named temporary nonimmigrant workers that can be included on a single H-2 petition, despite the processing time requirement.

OIG found that the flat fee structure has created disparities in the costs employers pay to bring foreign workers into the United States and be more burdensome for small employers or others who petition to bring in a single worker for whom the fee exceeds the processing cost as compared to large petitioners. Conversely, employers seeking to bring in multiple named workers pay disproportionately less as their petitions can be labor intensive, taking days and sometimes weeks to complete. Large petitions are complex and error prone when adjudicators rush to process them within required time frames. Prompt USCIS action to assess a more equitable fee structure or limit the number of named workers listed per petition would help eliminate disparate costs to employers, reduce the potential for errors, and better align agency processing costs.

DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Redacted)

Number: OIG-17-40
Date: 3/20/2017
Summary: Following the December 2015 terrorist attack in San Bernardino, California, Congress raised concerns about the use of social media by terrorist groups and requested that DHS expand social media background checks. DHS established a task force for using social media to screen applicants for immigration benefits. In connection with that effort, USCIS began pilots to expand social media screening of immigration applicants. Additionally, ICE independently began a pilot to use social media screening during the visa issuance process.

According to OIG, these pilots, on which DHS plans to base future department-wide use of social media screening, lack criteria for measuring performance to ensure they meet their objectives. Although the pilots include some objectives, such as determining the effectiveness of an automated search tool and assessing data collection and dissemination procedures, it is not clear DHS is measuring and evaluating the pilots' results to determine how well they are performing against set criteria. Because components are not measuring their pilots against clear success criteria, DHS may not be able to make informed decisions when it designs its social media screening program and implements a department-wide future social media screening program.

Individuals with Multiple Identities in Historical Fingerprint Enrollment Records Who Have Received Immigration Benefits

Number: OIG-17-111
Date: 9/25/2017
Summary: In response to a congressional request, OIG examined USCIS' data set of aliens whose fingerprints had been uploaded into the Automated Biometric Identification System (IDENT) through Historical Fingerprint Enrollment (HFE I) to determine how many aliens with multiple identities whose fingerprints were digitized and uploaded into IDENT received immigration benefits. From this data set, OIG determined that, as of April 24, 2017, 9,389 aliens USCIS

identified as having multiple identities had received an immigration benefit. When taking into account the most current immigration benefit these aliens received, OIG found that naturalization, permanent residence, work authorization, and temporary protected status represent the greatest number of benefits, accounting for 8,447 or 90 percent of the 9,389 cases. Benefits approved by USCIS for the other 10 percent of cases, but not discussed in this report, include applications for asylum and travel documents. According to USCIS, receiving a deportation order or having used another identity does not necessarily render an individual ineligible for immigration benefits.

OIG found that USCIS has drafted a policy memorandum, Guidance for Prioritizing IDENT Derogatory Information Related to Historical Fingerprint Enrollment Records (draft policy memo), outlining how it will review cases of individuals with multiple identities whose fingerprints were uploaded into IDENT through HFE. Per the draft policy memo, USCIS will prioritize cases for review according to the type of approved immigration benefit. USCIS will take appropriate action if it determines the individual engaged in fraud or willful misrepresentation, or obtained the benefit unlawfully, and is not subject to an exception or eligible for a waiver. Actions include rescinding, revoking, or terminating an immigration benefit, and/or initiating removal proceedings; or referring the case to the appropriate enforcement authority (i.e., ICE or DOJ). USCIS will not take action if it determines the alien was eligible for the benefit.

U.S. Coast Guard (USCG)

GAO Reports

Coast Guard Cutters: Depot Maintenance Is Affecting Operational Availability and Cost Estimates Should Reflect Actual Expenditures

Number: GAO-17-218
Date: 3/2/2017
Summary: Maintenance work for the Fast Response Cutter (FRC) and National Security Cutter (NSC) has lowered the operational availability of each fleet. Although both cutters on average have met their minimum mission capable targets over the long term, increased depot maintenance has more recently reduced each cutter's rates below targets. The FRC's rate is lower, in part, because of a series of unanticipated drydock periods to correct issues covered by its 12-month warranty. The NSC's lower rate is primarily because of anticipated 2-year maintenance and system upgrade periods performed on each newly delivered NSC. Both cutters have experienced problems with the diesel engines, which caused lost operational days and hindered operations while underway.
The U.S. Coast Guard has initiated design changes on the FRC and NSC, but some of the NSC's changes to address maintenance problems will not be installed until after each cutter is delivered. While the U.S. Coast Guard plans at least $17 million on FRC design changes, officials estimate the warranty has helped avoid $77 million for repaired systems. This includes about $52 million to replace 20 diesel engines that have degraded FRC operations since first discovered in July 2013. Design changes on the NSCs are expected to cost the U.S. Coast Guard at least $260 million. In order to maintain production schedules, several changes will be completed after delivery of each NSC, including the ninth NSC, which has not yet begun construction. Thus, systems with known deficiencies are being installed, only to be replaced later. Officials stated this approach is more cost

effective; however, the U.S. Coast Guard did not document its cost analyses, in accordance with GAO cost estimating best practices. Without such documentation, the U.S. Coast Guard cannot demonstrate that it is making cost-effective decisions.

Since 2010, depot maintenance expenditures for the FRC and NSC have been $106.6 million less than the U.S. Coast Guard estimated. This amount remains in a centrally managed account and is made available for other surface assets, such as aging, legacy vessels. U.S. Coast Guard officials stated that depot maintenance estimates are not adjusted or updated over the service life of an asset class. Periodically updating depot maintenance cost estimates—in accordance with GAO cost estimating best practices—for each asset class could provide decision makers with much needed information with which to determine future budgets.

Coast Guard Recapitalization: Matching Needs and Resources Continue to Strain Acquisition Efforts

Number: GAO-17-654T
Date: 6/7/2017
Summary: In order to meet its missions of maritime safety, security, and environmental stewardship, the U.S. Coast Guard employs a variety of surface and air assets, several of which are approaching the end of their intended service lives. As part of its efforts to modernize its surface and air assets (an effort known as recapitalization), the U.S. Coast Guard has begun acquiring new vessels, such as the National Security Cutter, Fast Response Cutter, and a number of air assets, and developing the Offshore Patrol Cutter. Despite the addition of new assets, concerns surrounding capability and affordability gaps remain.

This statement addresses (1) the capabilities provided by the newer U.S. Coast Guard assets, (2) maintainability and equipment challenges for the new cutters, and (3) the overall affordability of the U.S. Coast Guard's acquisition portfolio. This statement is based on GAO's extensive body of work examining the U.S. Coast Guard's acquisition efforts spanning several years, including the March 2017 report on the NSC and FRC's maintainability.

Coast Guard Acquisitions: Limited Strategic Planning Efforts Pose Risk for Future Acquisitions

Number: GAO-17-747T
Date: 7/25/2017
Summary: In June 2014, GAO found that the U.S. Coast Guard lacked long-term planning to guide the affordability of its acquisition portfolio and recommended the development of a 20-year fleet modernization plan to identify all acquisitions necessary for maintaining at least its current level of service and the fiscal resources necessary to build and modernize its planned surface and aviation assets. U.S. Coast Guard officials stated that they are developing a 20-year Capital Investment Plan (CIP), but the timeframe for completion is unknown. The U.S. Coast Guard does, however, submit a 5-year CIP annually to Congress that projects acquisition funding needs for the upcoming 5 years. GAO found the CIPs do not match budget realities in that tradeoffs are not included. In the 20-year CIP, GAO would expect to see all acquisitions needed to maintain current service levels and the fiscal resources to build the identified assets as well as tradeoffs in light of funding constraints.

As GAO reported in June 2016, the U.S. Coast Guard's heavy icebreaker fleet was operating at a reduced capacity with only one heavy polar icebreaker in service, resulting in limited access to both the Arctic and Antarctic regions year-round. The U.S. Coast Guard's only active heavy icebreaker, the Polar Star, is approaching the end of its expected service life, and the U.S. Coast Guard plans to implement a limited service life extension to keep it operational until the new icebreaker is available. An official cost estimate has not been completed, but the U.S. Coast Guard estimates this extension will cost roughly $75 million.

Consequently, the U.S. Coast Guard expedited its acquisition of new heavy icebreakers with delivery of the first polar icebreaker scheduled in 2023. This delivery schedule poses potential risk as the required acquisition documents may not be completed in time to award the contract in 2019, as currently scheduled. Further, in order to meet this accelerated schedule, the first polar icebreaker would need to be fully funded in fiscal year 2019 with a preliminary cost estimate of $1.15 billion, alongside the Offshore Patrol Cutter acquisition. The U.S. Coast Guard has not articulated how it will prioritize its acquisition needs given its Offshore Patrol Cutter is expected to absorb half to two-thirds of its annual acquisition funding requests—based on recent funding history—starting in 2018.

Coast Guard: Workforce Actions Under Way to Address Backlog in Recreational Vessel Documentation

Number: GAO-17-629
Date: 9/12/2017
Summary: The backlog for processing applications for recreational certificates of documentation increased after U.S. Coast Guard's National Vessel Documentation Center (NVDC) management modified the application review process in July 2010 by limiting the number of documentation officers available to process recreational applications. Other factors—including a prior reduction to recreational staffing levels in fiscal year 2009 as a result of decreases in recreational fee collections associated with the recession—also contributed to the backlog over time.

- December 2007 to June 2009—During the recession, NVDC's recreational fee collections decreased from $5.5 million in fiscal year 2007 to $3.6 million in fiscal year 2009.
- Fiscal year 2009—In response to decreased recreational fee collections, NDVC officials reduced the number of recreational officers from 27 to 10 to ensure recreational services were fully funded by recreational fee collections, as required by Department of Homeland Security (DHS) appropriations acts.
- July 2010—NVDC management implemented a control to ensure there were not more documentation officers reviewing recreational applications at any one time than there were filled recreational officer positions. NVDC did this to ensure full compliance with annual DHS appropriations acts, according to the NVDC director. Given that NVDC had 10 filled recreational officer positions at this time, this decision meant that a relatively small number of officers were available to process recreational applications—increasing the backlog.
- Fiscal years 2010 through 2014—NVDC was unable to reduce the backlog because recreational fee collections remained relatively flat and, as a result, NVDC was unable to increase the number of recreational officers to pre-recession levels because, according to

U.S. Coast Guard officials, doing so might have caused recreational costs to exceed recreational fee collections.

- November 2014 through June 2017—NVDC implemented a new fee that resulted in recreational collections doubling between fiscal years 2014 and 2016. Despite this fee increase, NVDC had not restored the number of recreational officers to pre-recession levels as of June 2017 primarily because of concerns about a change to the NVDC fee structure that may result from the U.S. Coast Guard Authorization Act of 2015. Specifically, the Act requires U.S. Coast Guard to issue a regulation to extend the time recreational certificates are valid from 1 to 5 years. NVDC relies heavily on collections from the annual renewal fee to fund recreational operations, and U.S. Coast Guard officials expressed concern about how changes to the renewal period and fee might affect recreational officer staffing levels.

NVDC has filled some vacant recreational documentation officer positions, is using overtime, and plans to restructure its workforce over the long-term to address staffing challenges. Regarding hiring, in June 2017 NVDC filled four vacant recreational documentation officer positions. Additionally, NVDC is using overtime in the short-term to address the backlog and plans to restructure its workforce over the long-term to ensure the appropriate mix of commercial and recreational staff.

Coast Guard: Status of Polar Icebreaking Fleet Capability and Recapitalization Plan

Number: GAO-17-698R
Date: 9/25/2017
Summary: Various responsibilities drive the U.S. Coast Guard's determination of its polar icebreaking mission requirements, and the U.S. Coast Guard has been unable to address all polar icebreaking requests since 2010. For example, the U.S. Coast Guard reported fulfilling 78 percent (25 of 32) of U.S. government agency requests for polar icebreaking services during fiscal year 2010 through 2016. U.S. Coast Guard officials cited various factors affecting the U.S. Coast Guard's ability to meet all requests, particularly the unavailability of its heavy polar icebreakers.

The U.S. Coast Guard has taken various actions to advance its heavy polar icebreaker acquisition program since establishing it in 2013, such as partnering with the Navy and engaging the shipbuilding industry, but faces risks in implementing its accelerated acquisition schedule. In particular, in October 2016, the U.S. Coast Guard released a notional schedule for the heavy polar acquisition program showing delivery of the first of three heavy polar icebreakers in fiscal year 2023--three years sooner than initially planned. However, U.S. Coast Guard officials reported that should acquisition planning documents, including acquisition and lifecycle cost estimates, not be completed and approved by the end of fiscal year 2017, the program may not be able to meet its schedule for releasing the request for proposals for detail design and construction (a key step in the acquisition process) in mid-fiscal year 2018. This may then delay the contract award scheduled for fiscal year 2019 and extend the proposed delivery date.

The U.S. Coast Guard plans to extend the service life of the Polar Star to bridge a potential heavy icebreaker capability gap, but has not completed assessments to determine the cost of the plan. According to U.S. Coast Guard planning documents, the U.S. Coast Guard faces a potential heavy polar icebreaker capability gap of up to three years between the end of the Polar Star's service life

and the scheduled delivery of the lead replacement heavy icebreaker in fiscal year 2023. While the U.S. Coast Guard considered various options to bridge this potential heavy icebreaker gap, in a January 2017 study the U.S. Coast Guard reported that it was planning for a limited service life extension of the Polar Star to keep it operational until fiscal year 2025, at an initial cost estimate of $75 million. However, the U.S. Coast Guard has not completed a formal cost estimate for this effort and we have previously reported that the $75 million estimate may be unrealistic. In keeping with OMB guidance on making decisions about federal programs, decisions about the limited service life extension should include comprehensive information about the benefits and costs associated with the planned upgrades, including its capability to meet operational objectives. In addition, cost estimating best practices should be used when developing the formal cost estimate. These best practices outline the steps that should be followed to develop a credible cost estimate to include, but are not limited to, conducting a risk and uncertainty analysis that accounts for the probability of risk occurrence. The U.S. Coast Guard would benefit from ensuring that it has completed its cost estimate before committing to this approach.

DHS OIG Reports

AMO and Coast Guard Maritime Missions Are Not Duplicative, But Could Improve with Better Coordination

Number: OIG-17-03
Date: 10/14/2016
Summary: Within DHS, CBP Air and Marine Operations (AMO) and the U.S. Coast Guard share responsibility for maritime security missions. At the request of Congress, the OIG reviewed the maritime missions and responsibilities of AMO and the U.S. Coast Guard.

The OIG found that the two components' maritime missions and responsibilities are not duplicative; their efforts bolster the overall effectiveness of DHS maritime border security and improve the ability to prevent the illegal flow of contraband and people into the country. Given the large area of responsibility, different activities, and limited resources, eliminating the maritime law enforcement responsibilities of either agency — or combining them — could be harmful to border security. However, AMO and the U.S. Coast Guard could improve coordination in some areas, which could potentially increase effectiveness of maritime border security, result in potential efficiencies, and enhance unity of effort.

Oversight Review of the US Coast Guard Investigative Service

Number: OIG-17-74-IQO
Date: 6/23/2017
Summary: The OIG conducted this review as part of the planned periodic review of the DHS component internal affairs offices by the DHS Office of Inspector General in keeping with the oversight responsibilities mandated by the Inspector General Act of 1978, as amended.

The review determined that significant issues with the agency's case management system prevented us from making substantive observations about the quality of their investigations. We noted issues with outdated policies and the absence of a Privacy Impact Assessment for the case management

system. Additionally, CGIS could not provide evidence to confirm whether employees complied with special agent training requirements. CGIS employees voiced concerns about trust in senior leadership and perceived questionable hiring practices. They also articulated a need for more resources.

U.S. Secret Service (USSS)

GAO Reports

No GAO reports were available that aligned to this Component.

DHS OIG Reports

The Secret Service Has Taken Action to Address the Classified Recommendations of the Protective Mission Panel

Number: OIG-17-47
Date: 3/16/2017
Summary: Following the September 19, 2014 White House fence jumping incident, the Secretary of Homeland Security established the Protective Mission Panel (PMP) to undertake a broad independent review of the Secret Service's protection for the White House Complex (WHC). In addition to recommendations made in an unclassified report, the PMP made a number of recommendations in its December 2014 classified report. As directed by Congress in the Consolidated Appropriations Act, 2016, the OIG reviewed the Secret Service's actions to address the PMP's classified recommendations. The PMP's classified recommendations primarily relate to security gaps and vulnerabilities at the WHC. The OIG reviewed changes made by the Secret Service to equipment, technology, and operations in response to these recommendations. The Secret Service has taken action to address the PMP's classified recommendations by using funding appropriated for PMP initiatives to begin enhancing security and refreshing technology at the WHC. As in the OIG's unclassified report, the OIG concluded that fully implementing many of the recommendations will depend on staff increases, sustained funding, and a multi-year commitment by Secret Service and Department leadership to ensure actions continue even during times of increased protective mission demands and unexpected priorities. In its response to this report, the Secret Service reiterated its agreement with our conclusion. The OIG made no additional recommendations in their report.

The Secret Service Has Taken Action to Address the Recommendations of the Protective Mission Panel

Number: OIG-17-10
Date: 11/10/2016
Summary: Following the September 19, 2014 White House fence jumping incident, the Secretary of Homeland Security established the Protective Mission Panel (PMP) to undertake a broad independent review of the United States Secret Service's protection of the White House Complex.

The PMP made 19 recommendations in its December 2014 unclassified report. The Secret Service has clearly taken the PMP's recommendations seriously, which it has demonstrated by making a number of significant changes. Specifically, it has improved communication within the workforce, better articulated its budget needs, increased hiring, and committed to more training. Using funding appropriated for PMP initiatives, the Secret Service has also begun enhancing security and refreshing technology at the White House Complex. However, fully implementing many of the PMP's recommendations will require long-term financial planning, further staff increases, consistent re-evaluation of the initiated actions' effectiveness, and a multi-year commitment by Secret Service and Department of Homeland Security leadership.

USSS Faces Challenges Protecting Sensitive Case Management Systems and Data

Number: OIG-17-01
Date: 10/7/2016
Summary: USSS did not have adequate protections in place on systems to which Master Central Index (MCI) information was migrated. USSS information technology (IT) management was ineffective, including inadequate system security plans, systems with expired authorities to operate, inadequate access and audit controls, noncompliance with logical access requirements, inadequate privacy protections, and over-retention of records. These problems occurred because USSS has not consistently made IT management a priority. The USSS Chief Information Officer (CIO) lacked authority for all IT resources and was not effectively positioned to provide necessary oversight. Inadequate attention was given to updating USSS IT policies to reflect processes currently in place. High turnover and vacancies within the Office of the CIO meant a lack of leadership to ensure IT systems were properly managed. In addition, USSS personnel were not adequately trained to successfully perform their duties. USSS initiated steps in late 2015 to improve its IT program, including centralizing all IT resources under a full-time CIO and drafting plans for an improved IT governance framework. However, until these improvements are implemented and can demonstrate effectiveness, USSS systems and data will remain vulnerable to unauthorized access and disclosure, and the potential for incidents similar to what the OIG investigated in 2015 will remain.

Component Acronyms

Below is the list of DHS Components and their Acronyms.

AO – Analysis and Operations
CBP – 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 – Immigration and Customs Enforcement
NPPD – National Protection and Programs Directorate
OHA – Office of Health Affairs
OIG – Office of Inspector General
S&T – Science and Technology Directorate
TSA – Transportation Security Administration
USCG – U.S. Coast Guard
USCIS – U.S. Citizenship and Immigration Services
USSS – U.S. Secret Service

Homeland
Security

Homeland
Security