

Major Management and Performance Challenges Facing the Department of Homeland Security






OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

November 9, 2018

MEMORANDUM FOR: The Honorable Kirstjen M. Nielsen
Secretary
Department of Homeland Security

FROM: John V. Kelly 
Senior Official Performing the
Duties of the Inspector General

SUBJECT: *Major Management and Performance Challenges Facing
the Department of Homeland Security*

For your information is our annual report, *Major Management and Performance Challenges Facing the Department of Homeland Security*. Pursuant to the *Reports Consolidation Act of 2000*, the Office of Inspector General is required to issue a statement that summarizes what the Inspector General considers to be the most serious management and performance challenges facing the agency and briefly assess the agency's progress in addressing those challenges. This requirement is consistent with our duties under the *Inspector General Act* to conduct audits, as well as provide leadership and recommend policies to promote economy, efficiency, and effectiveness in Department of Homeland Security programs and operations.

We acknowledge past and ongoing efforts by Department's senior leadership to address the challenges identified in this report. At the same time, our aim in this report is two-fold — to identify areas that need continuing focus and improvement and to point out instances in which senior leadership's goals and objectives are not executed throughout the Department. Therefore, we highlight persistent management and performance challenges that hamper the Department's efforts to accomplish the homeland security mission efficiently and effectively. The Department continues to strive to act as a single, focused organization while establishing strong internal controls and incorporating management fundamentals. DHS also faces challenges with overseeing and managing critical aspects of the homeland security mission, as well as acquisitions and cybersecurity.

Overcoming these management and performance challenges demands unified action. The Department has taken steps to achieve this unity, such as starting an Immigration Data Integration Initiative and establishing a requirements process that moves from program-specific requirements to those focused on broader capabilities. However, the challenge persists. A lack of coordination and harmony can negatively affect all aspects of DHS' programs and operations



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

— planning, acquisition, budgeting, and execution. To efficiently and effectively fulfill its vital mission of protecting and securing our Nation, the Department must work cohesively.

Unified Effort, Internal Controls, and Management Fundamentals

Since its creation 15 years ago, DHS' overriding and continuing challenge remains building a single, cohesive, and effective organization greater than the sum of its parts — the very reason it was established. Reaching this goal demands effective collaboration and integration of a wide array of component management functions, programs, and operations, all aimed at accomplishing a multi-faceted homeland security mission. The Department has not yet demonstrated it can take a unified approach, while implementing effective internal controls and incorporating management fundamentals in programs and operations across components. The current environment of relatively weak internal controls and management fundamentals affects all aspects of the Department's mission, from border protection and immigration enforcement to protection against terrorist attacks and natural disasters.

Our recent work offers examples of the Department's challenges effectively overseeing and managing programs and operations through careful planning; gathering complete and reliable data for informed decision making; implementing and enforcing clear and consistent policies, procedures, and practices; and establishing meaningful performance measures for future improvement.

Lack of Planning

In a review of U.S. Immigration and Customs Enforcement's (ICE) 287(g) program, ICE approved 40 additional applicants without planning for a corresponding increase in program management staffing, determining how to promptly deliver needed information technology (IT) equipment to participants, or ensuring participants are fully trained. Specifically, ICE did not analyze program needs to determine how many additional 287(g) program managers should be hired and was not able to hire enough to keep up with the quick expansion. Approving all new participants without adequate planning has hindered ICE's oversight and management of the 287(g) program and may be affecting participating agencies' ability to assist ICE in enforcing immigration laws and identifying removable aliens.¹

Following our investigation of U.S. Customs and Border Protection's (CBP) implementation of the January 2017 Executive Order 13769, *Protecting the Nation from Foreign Terrorist Entry into the United States* (EO), we determined

¹ [*Lack of Planning Hinders Effective Oversight and Management of ICE's Expanding 287\(g\) Program \(OIG-18-77\)*](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

that CBP was caught by surprise when the President issued the EO.² DHS had little opportunity to prepare for and respond to basic questions about the categories of affected travelers. We also observed that the lack of a public or congressional relations strategy significantly hampered CBP and harmed its public image.

Incomplete and Unreliable Data

As noted in an audit of the Department's controls over firearms and other sensitive assets, the Department did not have complete and accurate property management data for effective oversight and informed decision making. Those responsible for managing the Department's sensitive assets must know the total number across all components. Yet, the system used to manage these assets did not contain complete and accurate information. Without Department oversight and policy improvements, highly sensitive assets will continue to be subject to loss or theft and the safety of the general public will be at risk.³

The *Digital Accountability and Transparency Act of 2014* requires DHS to submit complete, accurate, and timely spending data to the Department of the Treasury for publication on USASpending.gov. Although DHS met the Act's mandated submission deadline, we identified issues with the completeness and accuracy of its first data submission, which hindered the quality and usefulness of the information. DHS has improved its data reconciliation procedures since making its first quarterly submission to Treasury and should continue to reconcile misalignments, identify errors and unacceptable timing differences, and develop or adjust existing internal controls to improve the overall quality of its data.⁴

Based on our observations in the field, we determined that DHS was not fully prepared to implement the Administration's Zero Tolerance Policy or to deal with some of its after-effects.⁵ Among other challenges, DHS had difficulty identifying, tracking, and reunifying families separated under the Zero Tolerance Policy due to limitations with IT systems, including a lack of integration among ICE's, CBP's, and Department of Health and Human Services' systems. DHS struggled to provide accurate, complete, reliable data on family separations and reunifications, raising concerns about the accuracy of its reporting.

² [*DHS Implementation of Executive Order #13769 "Protecting the Nation From Foreign Terrorist Entry Into the United States"* \(OIG-18-37\)](#)

³ [*DHS' Controls Over Firearms and Other Sensitive Assets* \(OIG-18-05\)](#)

⁴ [*DHS' Implementation of the DATA Act* \(OIG-18-34\)](#)

⁵ [*Special Review - Initial Observations Regarding Family Separation Issues Under the Zero Tolerance Policy* \(OIG-18-84\)](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Unclear and Unenforced Policies, Procedures, and Practices

Following our department-wide review of conduct and discipline, we concluded that DHS' support components do not have sufficient processes and procedures to address misconduct.⁶ These deficiencies exist because no single office or entity is responsible for managing and overseeing misconduct issues across support components. Without comprehensive department-wide procedures, DHS cannot ensure the components address allegations properly or administer disciplinary actions consistently.

At four of five ICE detention facilities inspected, OIG identified issues that raised concerns about management's failure to ensure the contracted facilities complied with policies and procedures in detention standards. For example, some detainees were housed incorrectly based on their criminal history; others were strip searched in violation of standards; and staff did not always use available language services to facilitate communication with detainees. Some facility staff reportedly deterred detainees from filing grievances and did not thoroughly document resolution of grievances. The problems we identified undermine the protection of detainees' rights, their humane treatment, and the provision of a safe and healthy environment.⁷

After reviewing ICE's two types of inspections for detention facilities, we reported that one type of inspection does not fully examine actual conditions or identify all deficiencies and the other type is too infrequent to ensure facilities correct all deficiencies. Moreover, ICE does not adequately follow up on identified deficiencies or consistently hold facilities accountable for correcting them, which further diminishes the usefulness of the inspections.⁸

In our special review of DHS' implementation of the Zero Tolerance Policy, we observed that, faced with resource limitations and other challenges, DHS regulated the number of asylum-seekers entering the country through ports of entry at the same time that it encouraged asylum-seekers to come to the ports, which may have caused more illegal border crossings.

Inadequate Performance Measures

During our assessment of the Federal Air Marshal Service's (FAMS) contributions to the Transportation Security Administration's layered approach to security, we determined that FAMS lacked performance measures for 24 strategic initiatives and most ground-based activities outlined in its strategic plan. Additionally, performance measures for FAMS' Visible Intermodal

⁶ [*DHS Support Components Do Not Have Sufficient Processes and Procedures to Address Misconduct \(OIG-18-81\)*](#)

⁷ [*Concerns about ICE Detainee Treatment and Care at Detention Facilities \(OIG-18-32\)*](#)

⁸ [*ICE's Inspections and Monitoring of Detention Facilities Do Not Lead to Sustained Compliance or Systemic Improvements, \(OIG-18-67\)*](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Prevention and Response Team operations failed to determine their effectiveness. FAMS could not provide a budget breakout by division or operational area. Without effective performance measures or detailed accounting of funds, FAMS cannot ensure it is maximizing its resources to address its highest risks and cannot measure the value of its investments in its ground-based activities.⁹

In automating naturalization benefits delivery, U.S. Citizenship and Immigration Services (USCIS) lacked performance measures to assess whether its IT system was achieving the expected outcomes to improve efficiency, accuracy, and security in benefits delivery.¹⁰ Existing performance measures were neither clear nor focused. Although USCIS collected a number of metrics to monitor system performance, it did not monitor the operational impact or quality of automated benefits processing. For example, it could not measure whether it had achieved targets for reducing adjudication time and the use of paper to process immigration benefits. In response to our recommendation, USCIS provided evidence that it had defined qualitative and quantitative metrics for each program goal.

DHS' Efforts to Strengthen Internal Controls

Recognizing that the U.S. Government Accountability Office (GAO) and OIG continue to identify internal control issues that profoundly affect reporting of accurate, reliable financial and programmatic information, the Department has taken steps to strengthen its internal controls. For example, DHS has established an internal control reporting structure, which allows the Secretary to report and provide reasonable assurance on the effectiveness of the Department's system of internal controls. DHS and its components also continue to establish, monitor, and implement corrective actions to eliminate weaknesses related to IT controls and financial reporting. Many components have implemented plans to assess the effectiveness of operational internal controls through inspections, evaluations, and desk audits. Finally, in FY 2018, among other actions, DHS updated its risk profile and developed an operational risk register at each component.

Oversight and Management of the Homeland Security Mission

Our recent reviews illustrate how critical it is for the Department to effectively oversee and manage various aspects of the homeland security mission, including disaster assistance, border protection, transportation security, and immigration enforcement. Specifically, the Department has had difficulty overseeing disaster assistance grants and grantees, as well as managing the National Flood Insurance Program. DHS also faces challenges safeguarding

⁹ [*FAMS Needs to Demonstrate How Ground-Based Assignments Contribute to TSA's Mission \(OIG-18-70\)*](#)

¹⁰ [*USCIS Has Been Unsuccessful in Automating Naturalization Benefits Delivery, \(OIG-18-23\)*](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

controlled areas and systems, protecting our borders against illegal entry of contraband, efficiently screening international travelers, and ensuring applicants for immigration benefits are both protected and meet requirements. These challenges also touch on tangential issues, such as the opioid crisis and public health.

Disaster Assistance

Recent hurricanes, wildfires, and other events highlight the Federal Emergency Management Agency's (FEMA) challenges responding to natural and manmade disasters — in both immediate response and long-term recovery efforts. FEMA continues to face systemic challenges managing its disaster assistance grant programs. On average, FEMA awards about \$10 billion each year in disaster assistance grants and preparedness grants. The 2017 hurricane season was the costliest in U.S. history. Three major hurricanes — Harvey, Irma, and Maria — made landfall in 4 weeks during August and September 2017. During this timeframe, the President declared seven major California disasters eligible for FEMA Public Assistance Program funding. As historic and unprecedented disasters continue to strike, the Department and FEMA must address significant challenges, which, unmitigated, will continue to delay recovery efforts and put billions of dollars of Federal funds at risk.

We issued a special report to FEMA leadership regarding the potential procurement challenges that would likely arise during the recovery phases of Hurricanes Harvey, Irma, and Maria — with damage estimates in excess of \$300 billion.¹¹ We reported that the massive scale of damage and the large number of high dollar contracts that grantees and subgrantees would likely award translated to a significant risk that taxpayer monies might be spent on ineligible costs.

In a recent management alert, we reported that FEMA's guidance for post-disaster debris monitoring still lacks sufficient information to ensure adequate oversight.¹² In response to a 2011 DHS OIG report, FEMA released additional criteria for debris estimating and monitoring to enhance the overall effectiveness of debris operations. However, in January 2016, FEMA issued its *Public Assistance Program and Policy Guide*, which superseded selected Public Assistance Program guidance, including guidance for debris operations. The guide eliminates Federal and state monitoring responsibilities for debris operations and relies solely on subrecipients to monitor debris removal operations. Although local officials said contractors monitor debris removal as required, FEMA, State, and subrecipients provided limited or no contractor oversight, and contractor employees lacked adequate training for monitoring.

¹¹ [*Lessons Learned from Prior Reports on Disaster-related Procurement and Contracting \(OIG-18-29\)*](#)

¹² [*Management Alert – Observations of FEMA's Debris Monitoring Efforts for Hurricane Irma \(OIG-18-85\)*](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Without adequate guidance and oversight of debris removal by FEMA, State officials, and subrecipients, there is increased risk of fraud, waste, and abuse of taxpayer money.

According to a GAO report, the 2017 hurricanes and wildfires highlighted some longstanding issues and revealed other emerging response and recovery issues.¹³ For example, the concurrent timing and scale of the disaster damages nationwide caused shortages in available debris removal contractors and delays in removing disaster debris — a key first step in recovery. In addition, FEMA's available workforce was overwhelmed by the response needs. FEMA officials noted that staff shortages and lack of trained personnel with program expertise led to complications in its response efforts.

Our recent work related to disaster assistance programs demonstrates FEMA's continuing challenges holding grant recipients accountable for managing disaster relief funds. Under the Public Assistance Program, states are required to monitor subgrantees' activities to ensure compliance with applicable Federal requirements. Yet, we continue to document the failure of grantees to fulfill basic grant management responsibilities. For example, as a result of an audit of \$7 million in Public Assistance Program funds awarded to Richland County, North Dakota, we determined funding totaling \$6.2 million was ineligible because the County did not have the legal responsibility for repairs to township roadways.¹⁴ In general, our audits show that the oversight intended to monitor the billions of dollars awarded by FEMA in disaster assistance grants is often ineffective and inefficient, as well as vulnerable to fraud, waste, and abuse. Therefore, FEMA must ensure the states effectively manage their disaster relief grants and monitor their subrecipients.

In addition to issues with grant management, we identified a number of other challenges to FEMA's programs and operations. For example, FEMA failed to address persistent issues with technology planning, governance, and system support challenges to effectively support its mission.¹⁵ Specifically, in 2015 we recommended the Chief Information Officer finalize key planning documents related to IT modernization, execute against those planning documents, fully implement an IT governance board, improve integration and functionality of existing systems, and implement component-wide acquisition, development, and operation and maintenance standards. In 2018, many of the issues we reported in prior years remain unchanged, with adverse impact on day-to-day operations and mission readiness. In another example, FEMA created the Sandy Claims Review Process (SCRCP), but did not rely on legislatively mandated controls designed to ensure appropriate payments to flood victims.

¹³ [2017 Hurricanes and Wildfires-Initial Observations on the Federal Response and Key Recovery Challenges \(GAO-18-472\)](#)

¹⁴ [Management Alert - FEMA Should Recover \\$6.2 Million in Public Assistance Funds for Disaster Repairs That Are Not the Legal Responsibility of Richland County, North Dakota \(OIG-18-09\)](#)

¹⁵ [Management Alert-Inadequate Progress in Addressing Open Recommendations from our 2015 Report, "FEMA Faces Challenges in Managing Information Technology" \(OIG-18-54\)](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

This resulted in policyholders receiving unsupported additional payments, excessive costs to operate the process, and time delays processing claims. As of December 1, 2017, a re-review of claims under the SCRP cost more than \$196 million and had offered policyholders an additional \$270 million for their claims.¹⁶

Protecting Controlled Areas and Systems, Securing the Border and Transportation System, and Complying with Immigration Laws

As a result of a recent audit, we determined that DHS still faces challenges implementing and managing requirements of the Homeland Security Presidential Directive-12 program, which could lead to unauthorized access to controlled areas and information systems.¹⁷ The Department has an effective process for issuing personal identity verification cards, but still faces challenges such as ensuring separated contractors' cards are terminated. In addition, the Department has made limited progress in regulating access to its facilities and systems. Finally, DHS has not independently verified components' reported compliance in implementing logical access controls on their unclassified information systems. As a result, DHS cannot ensure that only authorized employees have access to its controlled facilities and systems and individuals who misrepresent their identities could circumvent controls and harm people and assets. Potential unauthorized access to information systems could lead to loss, theft, or misuse of sensitive information.

We also reported that U.S. Customs and Border Protection's (CBP) ineffective processes and IT security controls to support air mail inspection operations at John F. Kennedy International Airport could hamper efforts to prevent prohibited items, including opioids, from entering the United States.¹⁸ Despite legislative requirements to systematically target and widely prevent illegal imports, CBP inspects only a limited number of the hundreds of thousands of pieces of incoming air mail each day, largely due to difficulty inventorying and locating targeted mail, as well as inadequate guidance, equipment, and resources. Further, international mail suspected of containing contraband is not physically controlled due to procedural, space, and technical limitations. This inspection environment could lead to stolen, misplaced, or improperly delivered mail; hazards for inspection personnel; and potentially lost or damaged evidence to support criminal cases. Given a lack of oversight, servers supporting CBP's mail inspection processes do not meet IT security control requirements, and not all of them are included in CBP's system inventory, making them vulnerable to potential attacks and operational disruptions.

¹⁶ [Unsupported Payments Made to Policyholders Who Participated in the Hurricane Sandy Claims Review Process, \(OIG-18-38\)](#)

¹⁷ [Department-wide Management of the HSPD-12 Program Needs Improvement \(OIG-18-51\)](#)

¹⁸ [CBP's International Mail Inspection Processes Need Improvement at JFK International Airport \(OIG-18-83\)](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Additionally we reviewed deficient cyber security controls that resulted in a January 2, 2017 outage of CBP's TECS, the principal system used by officers at the border to help screen and determine the admissibility of arriving persons. This prevented CBP from promptly processing arriving international passengers at airports.¹⁹ We also reported that CBP did not have an adequate test environment for TECS. Without being able to test system changes using 'real-life' scenarios, CBP would be at increased risk that TECS would experience future outages.

Finally, we determined that USCIS has inadequate controls for verifying that foreign nationals seeking lawful permanent residence status meet health-related standards for admissibility.²⁰ First, USCIS is not properly vetting the physicians it designates to conduct required medical examinations of these foreign nationals, and it has designated physicians with a history of patient abuse or a criminal record. This is occurring because USCIS does not have policies to ensure only suitable physicians are designated. Second, when reviewing these foreign nationals' required medical forms, USCIS Immigration Services Officers are accepting incomplete and inaccurate forms because they are not adequately trained and because USCIS does not enforce its existing policies. As a result of these deficiencies, USCIS may be placing foreign nationals at risk of abuse by physicians performing medical examinations. USCIS could also be exposing the U.S. population to contagious or dangerous health conditions from foreign nationals erroneously granted lawful permanent resident status.

Acquisition Program Management

Acquisition program management continues to be one of the Department's significant challenge areas. Every year, the Department spends billions of dollars on a broad range of assets and services — from ships, aircraft, surveillance towers, and nuclear detection equipment to financial, human resources, and IT systems. Procurement practices that do not comply with Federal requirements can lead to high-risk contracts resulting in U.S. taxpayers bearing excessive and ineligible costs.

GAO also highlighted acquisition program management as one of DHS' high risk areas. According to GAO, DHS' efforts to improve its major acquisition programs are noteworthy, but the program continues to face challenges. Issues with staffing, funding, and defining the Department's requirements increase the likelihood that major acquisition projects will cost more and take longer than expected to complete. Components have an ongoing tendency to acquire systems before adequately defining requirements or developing performance measures.

¹⁹ [Review of CBP Information Technology System Outage of January 2, 2017 \(OIG-18-19\)](#)

²⁰ [USCIS' Medical Admissibility Screening Process Needs Improvement \(OIG-18-78\)](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Acquisition program management is inherently complex and high risk. It is further challenged by the magnitude and diversity of the Department's procurements, the need to expand capabilities to meet evolving threats, and budget constraints. DHS' well-documented challenges in this area cover decisions on a wide array of high-value goods and services. For example, in the past, although DHS has undertaken numerous initiatives to better manage the billions of dollars in IT investments, these projects frequently incur cost overruns and schedule slippages while contributing little to mission-related outcomes. We are currently auditing acquisition activities related to the planned wall on the southern border, which will likely highlight continuing challenges.

Our fiscal year 2018 body of work illustrates these ongoing challenges. For instance, we reported that although the United States Coast Guard approved approximately \$1.8 billion in IT procurements between FYs 2014 and 2016, it does not know if almost 400 information systems are receiving proper acquisition oversight.²¹ This occurred because the Coast Guard's controls over IT investments lack synergy and create weaknesses that affect its ability to adequately identify, designate, and oversee non-major IT acquisition programs. Programs that do not receive adequate oversight are at risk of wasting money, missing milestones, and failing to meet performance requirements.

As previously reported, the Department also faced challenges in managing its acquisition of the Performance and Learning Management System (PALMS).²² Because the PALMS program office did not effectively implement its acquisition methodology and did not monitor contractor performance, PALMS did not address the Department's critical need for an integrated, department-wide learning and performance management system. We are continuing audit work on PALMS.

Acquisition program management is critical to fulfilling all DHS' missions. The Department has taken steps to improve its processes and strengthen its oversight of major acquisition programs. However, to be fully successful, DHS must act as one entity working toward a common goal. The Department must continue toward a strong central authority and uniform policies and procedures to ensure lasting change.

Cybersecurity

Cybersecurity is an area of increasing risk throughout the Federal government. External threats such as hackers, cyber-terrorist groups, and denial of service attacks are of particular concern. GAO has identified the security of cyber assets and the privacy of personally identifiable information as another area on its High Risk List. GAO first designated information security as a government-

²¹ [Coast Guard IT Investments Risk Failure Without Required Oversight \(OIG-18-15\)](#)

²² [PALMS Does Not Address Department Needs \(OIG-17-91\)](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

wide high-risk area in 1997. This was later expanded to include protecting cyber critical infrastructure, as well as the privacy of personally identifiable information. The risks to these systems are increasing as security threats evolve and become more sophisticated. The Department must remain vigilant in establishing a control environment to continuously monitor potential IT risks, threats, and vulnerabilities.

Since its inception, the Department has struggled to implement and enforce a strong internal control environment that will protect the security of its information systems, critical infrastructure, and protecting the privacy of personally identifiable information. For example, CBP did not implement information security controls and safeguards to protect the information collected on its Unmanned Aircraft Systems (UAS).²³ CBP did not perform a privacy threshold analysis for the Intelligence, Surveillance, and Reconnaissance (ISR) Systems used in the UAS. Without a privacy assessment, CBP could not determine whether the system contained data requiring safeguards per privacy laws, regulations, and DHS policy. In addition, CBP did not implement adequate controls to limit physical access to the ground control station housing ISR Systems data. These information security deficiencies occurred because CBP did not establish an effective program structure, including the leadership, expertise, staff, training, and guidance needed to manage ISR Systems effectively. As a result, ISR Systems and mission operations were at increased risk of compromise by trusted insiders and external sources.

The Department also faces challenges to sharing cyber threat information across Federal and private sector entities.²⁴ The system DHS currently uses to share cybersecurity information does not provide the quality, contextual data needed to effectively defend against ever-evolving threats. Without acquiring a cross-domain information processing solution and automated tools, DHS cannot analyze and share threat information expeditiously. Further, without enhanced outreach, DHS cannot increase participation and improve coordination of information sharing across the Federal and private sectors.

We also identified examples of weak cybersecurity controls in a report on DHS' information security program. As a result of our review, we determined the Department could protect its information and systems more fully and effectively.²⁵ Specifically, in three of five areas, DHS' information security program fell one level below the targeted "Level 4" in the FY 2017 *Federal Information Security Modernization Act* reporting instructions. Among other issues, DHS lacked valid authority to operate 64 systems, did not implement all configuration settings required to protect component systems, did not monitor software licenses for unclassified systems, and did not test all system

²³ [CBP Has Not Ensured Safeguards for Data Collected Using Unmanned Aircraft Systems \(OIG-18-79\)](#)

²⁴ [Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015 \(OIG-18-10\)](#)

²⁵ [Evaluation of DHS' Information Security Program for FY 2017 \(OIG-18-56\)](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

contingency plans. In addition, based on the maturity model in this year's reporting instructions, DHS' information security program for intelligence systems was not effective.²⁶ Specifically, DHS' continuous monitoring tools were not interoperable, and it did not have documented procedures, formal training, or qualitative and quantitative measures to continuously monitor intelligence systems. Based on information provided by the Office of Intelligence and Analysis, OIG agreed to close our recommendations.

DHS depends on its systems and data to carry out its mission. Additional oversight is needed to address deficiencies. Otherwise, DHS cannot ensure its systems adequately protect the sensitive data they store and process. The Department must act as a central oversight body and ensure components secure these high-risk networks and comply with all applicable laws and regulations. Failure to do so increases the risk of unauthorized access manipulation, and misuse of the data they contain.

Looking Forward: Our Work Ahead

Although the Department continues to address and implement our recommendations to improve its programs and operations, these challenges highlight our need to continue proactive and thorough oversight, as well as the necessity for sustained effort by the Department. As agents of positive change, we strive to help the Department overcome these challenges by identifying them and making recommendations to improve efficiency and effectiveness; strengthen programs and operations; and safeguard public funds from fraud, waste, and abuse.

Management Comments and OIG Response

The Department's response to our report is attached as Appendix A. While the Department believes it has overcome many of its challenges, it is our assessment that while some improvements have been made, significantly more needs to be done. In response to the Department's comments, we did modify portions of our report to highlight positive actions taken by the Department.

²⁶ [Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems \(OIG-18-59\)](#)




OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
DHS' Comments to the Draft Report



October 29, 2018

MEMORANDUM FOR: John V. Kelly
Senior Official Performing the Duties of the
Inspector General
Office of Inspector General

FROM: Jim H. Crumacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office 

SUBJECT: Management Response to OIG's Draft Report: "Major
Management and Performance Challenges Facing the
Department of Homeland Security" (OIG-19-XXX, dated
October 19, 2018)

Thank you for the Office of Inspector General's (OIG) independent perspective on the most serious management and performance challenges facing the Department of Homeland Security (DHS). DHS senior leadership continues to maintain a culture where everyone understands and believes that audits make the Department stronger, by helping make our programs, operations, and activities more effective and efficient, thus ensuring our Nation and its citizens are safe, secure, and resilient against terrorism and other hazards.

The OIG's report provides valuable insights; however, the Department is concerned the report does not seem to equitably balance the challenges the Department faces with the progress made in addressing those challenges. Many of the summaries of prior OIG work in the report are outdated and do not reflect the current state of actions taken, ongoing, or planned to address the issues identified. For example, the summary about OIG's report on efforts to automate benefits processing using the Electronic Immigration System (ELIS), issued nearly one year ago,¹ does not recognize the significant progress U.S. Citizenship and Immigration Services (USCIS) has made establishing performance measures to assess whether ELIS is achieving expected outcomes related to improving efficiency, accuracy, and security in benefits delivery, even though credit for such progress in several instances was included in the report cited. In fact, OIG has already agreed to close four of the five recommendations made in this report, which confirms

¹ "USCIS Has Been Unsuccessful in Automating Naturalization Benefits Delivery," OIG-18-23 (Washington, D.C.: November 30, 2017)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

USCIS has implemented the agreed-upon actions and that doing so has corrected the deficiencies cited.

In addition, senior leadership believes that OIG's characterization of internal controls could leave readers of the report with a mistaken impression about DHS efforts and successes achieved in implementing effective internal controls and incorporating management fundamentals in programs and operations across Components, as it relates to the fulfillment of the Department's vital border security, immigration, law enforcement, and national preparedness missions, and protecting and securing our Nation. For example, the report does not recognize that DHS has established a robust internal control reporting structure, which enables the Secretary of Homeland Security to report and provide a reasonable assurance on the effectiveness of DHS's system of internal controls.

More specifically, "assurance statements" over the effectiveness of internal controls for financial reporting are based upon internal testing. Management performs an analysis on the pervasiveness and materiality over any identified deficiencies to determine their impact and management's analysis. Led by the DHS Chief Financial Officer (CFO), each Component and Under Secretary for Management assurance statements are reviewed for consideration and determination of impact to the DHS enterprise. Results of the analysis and recommendation for reporting are included in the overall DHS assurance statement, which is reviewed by the Secretary and Deputy Secretary prior to final publication. It is important to note that since FY 2006, DHS has reduced material internal control findings from ten to two. DHS and Components continue to establish, monitor and implement corrective actions to eliminate the remaining weaknesses related to IT controls and financial reporting.

Furthermore, many Components have also implemented an internal control plan to assess effectiveness of operational internal controls through inspections, self-evaluations, and desk reviews. In evaluating the results of internal control tests as well as a review of external audit reports and other sources of available information, none of the Component findings merited the Secretary of Homeland Security disclosing a material weakness in internal control over operations during the last four fiscal years. However, recognizing that U.S. Government Accountability Office (GAO) and OIG reports continue to identify internal control deficiencies, DHS and Components are persisting in their efforts to further implement and refine processes integrating and prioritizing control response and monitoring by maturing the Enterprise Risk Management framework at DHS. During FY 2018, DHS and Components have, in conjunction with DHS Office of the CFO, worked in coordination with the DHS Office of Policy (PLCY), DHS Risk and Analysis Executive Steering Committee, and others to (1) update the DHS risk profile through the Department's Strategic Review process, and (2) develop an operational risk register at each Component, among other activities.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Senior leadership is also concerned about OIG assertions regarding DHS efforts “to effectively oversee and manage programs and operations through careful planning; gathering complete and reliable data for informed decision making; implementing and enforcing clear and consistent policies, procedures, and practices; and establishing meaningful performance measures for future improvement.” Leadership acknowledges that while progress has been made, more work needs to be done in these areas; however, believes that OIG’s report discussion and characterization of the issues areas lacks context as regards the achievement of DHS’s strategic missions and goals.

For example, the DHS PLCY-led Immigration Data Integration Initiative has made progress on immigration data standards and sharing, the success of which has been demonstrated by strong Congressional support as signaled by additional appropriations provided to the Department. In addition, the DHS requirements process continues to mature and contribute to DHS acting as a single, focused organization. Most recently it has shown value in helping shape leadership decision-making on the U.S. Customs and Border Protection (CBP) Biometric Airport Exit Program, while working to coordinate CBP’s efforts with the Transportation Security Administration’s interest in expanding its use of biometrics in the airport environment. The requirements process has also made strides in moving from program-specific requirements to those focused on broader capability areas with the development of a suite of land and air domain awareness capability documents that will lead to better understanding of the contributions of existing domain awareness programs and more effective investment in future capability acquisitions in those areas. The start of a maritime domain awareness requirements effort is also imminent.

Also, GAO recently stated, after reviewing 28 acquisition programs, including DHS’s largest programs that were in the process of obtaining new capabilities, and programs GAO or DHS identified as at risk of poor outcomes, that “DHS is collecting more timely cost estimate information on its acquisition programs to make more informed investment decisions.”² For example, GAO found that the Department is regularly updating Life Cycle Cost Estimates (LCCEs), a GAO best practice that promotes accuracy.³ Specifically, all of the programs reviewed met DHS requirements to update their LCCE at each acquisition decision event, as applicable. In addition, 10 of 11 selected programs reviewed met DHS’s requirement for programs not yet in the deployment phase to update their LCCEs annually.

Further, GAO recognized that while DHS continues to face challenges in funding its acquisition portfolio, “to be clear, there can be valid reasons for cost growth or schedule

² GAO, “HOMELAND SECURITY ACQUISITIONS: Leveraging Programs’ Results Could Further Improve DHS’s Progress to Improve Portfolio Management,” GAO-18-339SP (Washington, D.C.: May 17, 2018).

³ GAO, “DHS PROGRAM COSTS: Reporting Program-Level Operations and Support Costs to Congress Would Improve Oversight,” GAO-18-344 (Washington, D.C.: April 25, 2018).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

delays.”⁴ For example, some programs are pursuing expanded capabilities to meet evolving threats and, in these situations, more time and money will be needed to achieve their ultimate goals. In addition, funding constraints can also impede a program’s intended delivery of capabilities. GAO stated that “DHS leadership has taken positive steps in recent years by strengthening its policies for acquisition management and resource allocations, and establishing policies related to requirements. Collectively, these policies reflect an integrated approach to managing investments.”⁵

At the Component level, CBP is advancing its requirements and performance measures approaches using its Capabilities Gap Assessment approach which informed their Border Security Improvement Plan (which is providing details and justification for the border wall construction). U.S. Immigration and Customs Enforcement also led a study during FY 2018 on “Empirical Modeling of Immigration Flows” to further develop its predictive analysis and performance management capabilities for detention bed space and workforce deployment (the model is called Policy Optimized Decision Support (PODS). PODS uses data from other DHS border security/immigration Components, as well as U.S. Department of Justice immigration data, and we expect that it will gain more widespread use by these other Components as it matures.

Overall, we disagree with OIG’s overall assessment that “Although DHS does attempt to address some of its challenges, it is generally not a sustained effort.” The fact is the Department is pouring more resources than ever before into effectively overseeing and managing programs and operations through careful planning; gathering complete and reliable data for informed decision making; implementing and enforcing clear and consistent policies, procedures, and practices; and establishing meaningful performance measures for future improvement to be a unified entity, and will continue to do so.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover for OIG consideration. Please contact me if you have any questions.

⁴ GAO, “HOMELAND SECURITY ACQUISITIONS: DHS Has Strengthened Management, but Execution and Affordability Concerns Endure,” GAO-16-338SP (Washington, D.C.: March 31, 2016).

⁵ GAO-18-339SP



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix B Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at:
www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General
Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.



OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305