

OFFICE OF INSPECTOR GENERAL

Major Management and Performance Challenges Facing the Department of Homeland Security



Homeland
Security

November 7, 2016
OIG-17-08



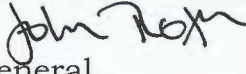
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

November 7, 2016

MEMORANDUM FOR: The Honorable Jeh C. Johnson
Secretary

FROM: John Roth 
Inspector General

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

Attached for your information is our annual report, *Major Management and Performance Challenges Facing the Department of Homeland Security*. We analyzed and incorporated the Department's technical comments as appropriate.

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 workforce; 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.

Unity of Effort

As in the past, DHS' primary challenge moving forward is transitioning from an organization of 22 semi-independent components, each conducting its affairs without regard to, and often without knowledge of, other DHS components' programs and operations, to a more cohesive entity focused on the central



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

mission of protecting the homeland. A lack of coordination and unity occurs in all aspects of DHS' programs — planning, programing, budgeting, and execution — and leads to waste and inefficiency.

Our previous audit and inspection reports are replete with examples of the consequences of failing to act as a single entity. Whether it is decisions on maintaining similar helicopters used by different components, harmonizing aviation maintenance management software, managing a vast vehicle fleet, coordinating protection of the maritime border, aligning immigration policies and data collection, sharing information, communicating on a common radio channel, or combatting tunnels on the Southwest border, DHS' challenges in this area are well documented. We are not alone in pointing out that the promise of a unified Department — the purpose of its creation — has not yet been realized. Congress, the Government Accountability Office, and interested third-party observers have all noted the challenge.

Progress has been made both in tone and substance. In the last 3 years, DHS leadership has taken steps to forge multiple components into a single organization. New policies and directives have been created to ensure cohesive budgeting planning and execution, including ensuring a joint requirements process. The Department also has a process to identify and analyze its mission responsibilities and capabilities, with an eye toward understanding how components fit together and how each adds value to the enterprise. A new method for coordinating operations, the Southern Border and Approaches Campaign, was created to try to reduce the silos and redundancy.

This progress has been the result of the force of will of a small team within the Department's leadership. Future leaders may not have the focus, capability, or desire to engage in the often coercive task of culture change. Unity of effort needs to be more than a slogan and an initiative. Ensuring continued progress requires the constant attention of senior leaders. Absent structural changes to ensure streamlined oversight, communication, responsibility, and accountability — changes that must be enshrined in law — the risk of DHS backsliding on the progress made to date is very real.

Employee Morale and Engagement

DHS is the third-largest Federal agency and its employees serve a variety of missions vital to the security of our nation. To achieve these missions, DHS must employ and retain people who are well prepared for their work and appropriately supported by their managers. Since its inception, however, DHS has suffered poor employee morale and a dysfunctional work environment.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

These issues are likely connected to challenges we repeatedly identify — the Department’s failure to develop, implement, and widely disseminate clear and consistent guidance; a lack of communication between staff and management; and insufficient training. DHS has also had problems determining how to assign staff appropriately and hiring and retaining enough people to handle a reasonable workload while maintaining a work-life balance. At times, DHS employees’ jobs are made more difficult by the lack of needed support, such as useful IT systems and up-to-date technology.

The Department spends about \$30 billion a year (40 percent of its budget) on employee salaries and benefits. Therefore, it is imperative that DHS leadership take all steps necessary to strengthen esprit de corps. The Partnership for Public Service has made recommendations to improve employee morale and engagement:

- Holding executives accountable for improving employee morale
- Partnering with employee groups to improve working relationships
- Designing and executing short-term activities to act on employee feedback and contribute to a potential long-term culture change
- Developing and committing to shared organizational values and aligning agency activities and employee interactions to those values
- Increasing transparency and connecting employees to the mission, the Department, and their co-workers
- Investing in and developing employees through leadership and technical training and by providing mentoring

The Secretary has made improving employee morale one of his top priorities and some progress has been made. The results of the 2016 Federal Employee Viewpoint Survey showed that, after 6 years of decline, employee engagement went up 3 percentage points — from 53 percent in 2015 to 56 percent this year. However, the Department continues to rank last among large agencies, which means leadership must sustain its focus on addressing this challenge.

Acquisition Management

Acquisition management, which is critical to fulfilling all DHS missions, is inherently complex, high risk, and challenging. Since its inception in 2003, the Department has spent tens of billions of dollars annually on a broad range of assets and services — from ships, aircraft, surveillance towers, and nuclear detection equipment to IT systems for financial management and human resources. DHS’ yearly spending on contractual services and supplies, along with acquisition of assets, exceeds \$25 billion. There continue to be DHS major acquisition programs that cost more than expected, take longer to deploy than



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

planned, or deliver less capability than promised. Although DHS has made much progress, it has not yet coalesced into one entity working toward a common goal. The Department still lacks uniform policies and procedures, a dedicated core of acquisition professionals, as well as component commitment to adhere to departmental acquisition guidance, adequately define requirements, develop performance measures, and dedicate sufficient resources to contract oversight.

For example, U.S. Citizenship and Immigration Services (USCIS) faces continuing challenges in its efforts to automate immigration benefits. After 11 years, USCIS has made little progress in transforming from paper-based processes to automated immigration benefits processing. Past automation attempts have been hampered by ineffective planning, multiple changes in direction, and inconsistent stakeholder involvement. USCIS deployed the Electronic Immigration System in May 2012, but to date customers can apply online for only 2 of about 90 types of immigration benefits and services. USCIS now estimates that it will take 3 more years—more than 4 years longer than estimated—and an additional \$1 billion to automate all benefit types as expected.

DHS has instituted major reforms to the acquisition process and has exerted significant leadership to gain control of an unruly and wasteful process. However, we worry that these reforms, if not continuously supported and enforced, could be undone. As DHS continues to build its acquisition management capabilities, it will need stronger departmental oversight and authority, increased commitment by the Department and components, as well as skilled personnel to effect real and lasting change.

Grants Management

The Federal Emergency Management Agency (FEMA) manages the Federal response to, and recovery from, major domestic disasters and emergencies of all types. In doing so, FEMA coordinates programs to improve the effectiveness of the whole community and leverages its resources to prevent, protect against, mitigate, respond to, and recover from major disasters, terrorist attacks, and other emergencies. In this role, FEMA awards an average of about \$10 billion each year in disaster assistance grants and preparedness grants.

Based on the results of OIG Emergency Management Oversight teams deployed to disaster sites in nearly a dozen states, we determined that FEMA generally responded effectively to disasters. Overall, FEMA responded proactively and overcame a variety of challenges while coordinating activities with other Federal agencies and state and local governments.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

However, our body of work over the past few years suggests that FEMA has not managed recovery from disasters well. Although FEMA provides grant management funding to grantees, FEMA has not held them accountable for managing subgrantees, and states and other grantees have not done well in guiding and managing subgrantees. This means the entire layer of oversight intended to monitor the billions of dollars awarded by FEMA in disaster assistance grants is ineffective, inefficient, and vulnerable to fraud, waste, and abuse. Of the \$1.55 billion in disaster grant funds we audited last year, we found \$457 million in questioned costs, such as duplicate payments, unsupported costs, improper procurement practices, and unauthorized expenditures. This equates to a 29 percent questioned-cost rate, which far exceeds industry norms, and it illustrates FEMA's continued failure to adequately manage grants.

We also saw examples of inadequate grant management in preparedness grants. In an overarching audit of OIG recommendations related to preparedness grants, we reported that FEMA had not adequately analyzed recurring recommendations to implement changes to improve its oversight of these grants. This occurred because FEMA did not clearly communicate internal roles and responsibilities and did not have policies and procedures to conduct substantive trend analyses of audit recommendations.

Although FEMA has been responsive to our recommendations for administrative actions and for putting unspent funds to better use, FEMA has not sufficiently held grant recipients financially accountable for improperly spending disaster relief funds. As of September 27, 2016, FEMA had taken sufficient action to close 130 of our 154 FY 2015 disaster grant audit report recommendations. However, the 24 recommendations that remained open contained 90 percent (\$413 million) of the \$457 million we recommended FEMA disallow that grant recipients spent improperly or could not support. Further, in FYs 2009 through 2014, FEMA allowed grant recipients to keep 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, minority, and women) to bid on federally funded work.

Based on our recurring audit findings, it is critically important that FEMA officials examine regulations, policies, and procedures and assess the need for more robust changes throughout all grant programs. FEMA should refocus its efforts to identify systemic issues and develop solutions to address the cause and not just the symptoms. FEMA needs to improve its oversight of state grantees and proactively engage with states to improve management and guidance of subgrantees. Nurturing positive relationships that emphasize



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

accountability for results and resource stewardship will set a clear tone for all stakeholders of FEMA grants.

Cybersecurity

Cybersecurity is a serious challenge, given the increasing number and sophistication of attacks against our Nation's critical infrastructures and information systems. In FY 2017, the Department requested \$1.6 billion to safeguard its complex mix of interconnected networks, legacy systems, web-based applications, and contractor-owned or operated systems that process, store, and share unclassified and classified information. Failure to secure these assets increases the risk of unauthorized access, manipulation, and misuse of the data they contain. External threats such as hackers, cyber-terrorist groups, and denial of service attacks are of particular concern.

Our annual *Federal Information Security Modernization Act of 2014* (FISMA) reviews show incremental DHS progress in establishing an enterprise-wide information security program. However, the Department is challenged to provide central oversight to make sure all components secure their networks. Over time, we have documented significant vulnerabilities, including

- Ensuring personal identity verification card implementation data, pursuant to Homeland Security Presidential Directive 12, is implemented and reported;
- Performing required weakness remediation reviews;
- Ensuring each system has a documented authority to operate;
- Taking adequate action to address security deficiencies;
- Implementing all DHS baseline configuration settings;
- Continuously maintaining information security programs;
- Continuously monitoring Secret and Top Secret systems; and
- Discontinuing use of unsupported operating systems (e.g., Windows XP and Windows Server 2003).

Under FISMA, DHS is also responsible for administering implementation of Office of Management and Budget information security policies and practices Federal government-wide. In line with this responsibility, DHS implemented EINSTEIN 1 and 2 to provide an automated process for collecting security information and detecting the presence of malicious activity on Federal networks. DHS has yet to deploy EINSTEIN 3 Accelerated across all Federal Government networks to expand intrusion prevention capabilities to counteract emerging threats. As the Government Accountability Office reported in January 2016, only 5 of 23 agencies were receiving intrusion prevention services, but DHS was working to overcome policy and implementation challenges. Further,



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

agencies had not taken all the technical steps needed to implement the system, such as ensuring that all network traffic is routed through EINSTEIN sensors. Within DHS, the National Protection and Programs Directorate has the overwhelming task of fulfilling the Department's national, non-law enforcement cyber security missions, as well as providing crisis management, incident response, and defense against cyber-attacks for Federal.gov networks.

We have identified inadequate protection of DHS components' sensitive systems and the data they contain. For example, due to inadequate controls, Secret Service employees were able to gain unauthorized access to the component's Master Central Index system containing Representative Chaffetz's personally identifiable information. DHS could better address insider threats by protecting against unauthorized removal of sensitive information via portable media devices and email, establishing processes for routine wireless vulnerability and security scans, and strengthening physical security controls to protect IT assets from possible theft, destruction, or malicious actions. More broadly, DHS components we audited could better ensure privacy of essential records, sensitive personally identifiable information, and intelligence information. Moreover, the Department could develop a strategic implementation plan, a training program, and an automated information sharing tool to enhance coordination among its components with cyber-related responsibilities.

Management Fundamentals

Although neither exciting nor publicly lauded, the basics of management are the lifeblood of informed decision making and successful mission performance. Management fundamentals include having accurate, complete information on operations and their cost; meaningful performance metrics on programs and goals; and appropriate internal controls. The Department has made strides in establishing its management fundamentals, including obtaining an unmodified opinion on its financial statements for the last 3 years. However, DHS still cannot obtain such an opinion on its internal controls over financial reporting. In plain terms, this means the Department can assemble reasonably accurate financial statements at the end of the fiscal year, but it has no assurance that its financial information is accurate and up-to-date throughout the year. DHS has also instituted many positive steps such as over-arching acquisition policies and other meaningful acquisition reforms, but the value of these steps is undermined by the lack of discipline in management fundamentals.

We have summarized the ongoing challenges the Department faces into three main categories, but caution that these challenges are both interrelated and cumulative:



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Collecting the Right Data

The Department does not prioritize collection of data in its program planning, does not always gather enough data, and does not validate the data it receives to ensure it is accurate and complete. The lack of reliable and complete data permeates through the entire Department and its components and is often accompanied by too little management oversight and weak internal controls. DHS leadership does not always assert its authority over the components to ensure it gets the data it needs when it needs it. As a result, DHS and the components often struggle making good decisions on acquisitions (what is needed and how much is needed) and correctly deploying resources (people, as well as acquired goods and services). Further, DHS does not have the data required to measure performance and use the feedback to adjust and improve programs and operations. We have identified numerous examples of this issue, including DHS' lack of accurate and complete inventory data for equipment, which hindered the provision of needed interoperable radio equipment, and incomplete inventory data on warehouse space, which led to wasted resources. In another example, neither the Department nor its components were collecting accurate data on the use of government vehicles and as a result could not accurately determine how many vehicles the components needed. Simply put, without the foundation of solid data, DHS cannot be certain it will achieve its mission and spend taxpayer dollars wisely and efficiently.

Collecting and Analyzing Cost Data

The Department, like most Federal Government agencies, does not put sufficient emphasis on collecting cost data for operations and programs. Successful businesses unfailingly track cost data because the cost of their operations or products directly impacts their bottom line revenue. Government does not have that bottom line drive for cost information; yet, all government programs rely on informed decision making to optimize performance. Without cost information, DHS is not prepared for reliable cost-benefit analysis of proposed program or policy changes or new initiatives. Because it does not fully understand the costs of its program choices, the Department is not equipped to analyze its risk decisions. The lack of information on program costs also limits basic investment decisions among competing programs. Our FY 2015 audit of U.S. Customs and Border Protection's (CBP) unmanned aircraft system program highlighted CBP's failure to capture complete cost data for the program. CBP did not include all the actual operating costs because some costs were paid from a different budget line item or program. We



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

determined that CBP was dramatically underestimating the cost of the program, at the same time it was considering expanding the program. Program decisions based on inaccurate or incomplete cost analysis can lead to program failure, poor performance, or significant delays. Since we issued our audit report, DHS has made substantial progress towards developing a common flying hour program.

Performance Measurement

A famous business axiom states, “what’s measured, improves,” but DHS does not routinely establish meaningful performance measures for many of its ongoing initiatives and programs. Multiple audit and inspection reports identify deficiencies in or the absence of DHS performance measures. Our audits have identified costly programs that DHS has not measured for effectiveness. Therefore, we do not know whether the investment of taxpayer resources is a good one. For example:

- The Transportation Security Administration (TSA) has continued to invest in its Screening of Passengers by Observation Techniques program without valid performance metrics to evaluate whether the investment is yielding appropriate results. In fact, 3 years after our initial audit, we found that TSA still is unable to determine its effectiveness.
- CBP’s Streamline, an initiative to criminally prosecute individuals who illegally enter the United States, had flawed measures of effectiveness and did not capture an accurate picture of the alien’s crossing history, re-entry, or re-apprehension over multiple years. As a result, CBP did not have good information to make management decisions about widening, maintaining, or constricting Streamline’s parameters.

Reliable and relevant feedback on program performance is critical to ensuring the Department does not invest its resources on unproductive, inefficient, or ineffective programs and initiatives.

These critical business fundamentals, unglamorous as they may be, are part of any mature and functioning government enterprise. The key to a more effective and efficient DHS is to focus on these basic government business practices. DHS achieved its unmodified opinion on the financial statements through concentrated hard work and attention to detail at every level of the Department. Similar emphasis must be placed on mastering the fundamentals of business management before the Department can fully mature as a world class organization.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
DHS Comments to the Draft Report


U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

November 1, 2016

MEMORANDUM FOR: John Roth
Inspector General
Office of Inspector General

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

SUBJECT: Draft OIG Report, "Major Management and Performance
Challenges Facing the Department of Homeland Security"
(Project No. 17-014-IQO-MGMT)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates having the Office of Inspector General (OIG) perspective on the most serious management and performance challenges facing the Department.

DHS is extremely proud of the open and transparent relationship it has with the OIG. As Secretary Jeh Johnson has said, "The IG serves an important role in helping the Department prevent and detect fraud, waste, mismanagement, and abuse." Within the Department, we believe that audits truly do help make us better, and thus we are committed to collaboratively working with the dedicated professionals that comprise the OIG.

For example, earlier this year the Senate Appropriations Committee praised DHS cooperation with OIG during the FY 2017 budget mark-up. Specifically, when commenting on "Inspector General Access" the Committee stated: "The Committee appreciates the leadership demonstrated by the Secretary and the Department's management team in ensuring full cooperation with OIG. Across the executive branch, the cooperation level is not as robust as it should be, as is required by law, nor as robust as it is at DHS."

By continuing to work collaboratively in an appropriate manner which respects the unique, independent status that OIG occupies within the Department, we will continue to make DHS better with each passing day. As our new mission statement reads, "With honor and integrity, we will safeguard the American people, our homeland, and our values."



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Challenge #1: Unity of Effort

As the draft report notes, “progress has been made both in tone and substance” in this area. One of Secretary’s Johnson’s top recommendations for the new DHS leadership team is to continue the management reform that began under his leadership, referred to as the “Unity of Effort Initiative.” This initiative, established in April 2014, is intended to break silos and centralize senior decision-making at DHS. New forums of transparency include DHS-wide joint activities, such as the Senior Leaders Council, Deputy’s Management Action Group, the Joint Requirements Council, and Joint Task Forces. These activities enhance pre-existing business management processes, linking strategic guidance to operational results as an enterprise, rather than as a set of Components, while also increasing Departmental effectiveness and efficiency. The Department continues to focus Unity of Effort to sustain and improve actions along the following lines of effort: (1) strengthening business management across the Department; (2) enhancing coordinated Departmental operations; (3) growing external partnerships; and (4) building a collaborative, joint DHS culture.

Challenge #2: Employee Preparedness and Morale

As the draft report notes, “The Secretary has made improving employee morale one of his top priorities and some progress has been made.” Improving DHS’ morale has been one of the Secretary’s top priorities, as evidenced by the aggressive campaign that he and Deputy Secretary Alejandro Mayorkas conducted across our 22 Component, 232,000 person workforce. The Secretary and Deputy Secretary have led by example, in part, by traveling across the country to speak to employees and thank them for their service. The Deputy Secretary established an Employee Engagement Steering Committee, chaired by the Under Secretary for Management and made up of senior executives from across DHS who collaborate on enterprise-wide solutions and share best practices and ideas for more local solutions. DHS also empowered its Components to be innovative and proactive with their engagement initiatives thru the development of component-specific action plans, and have created a “loop of accountability” with them so that we know where they are making progress as well as where they might need support in more challenging areas. This enables Components to focus on local engagement issues targeting solutions at the lowest level appropriate in order to have the best outcomes possible.

DHS also enhanced its two-way communications so that employees have a better sense of being connected to the DHS Mission, their respective Component’s mission, and to one another’s work. As a result, DHS saw improvements in overall 2016 Federal Employee Viewpoint Survey (FEVS) scores and the Engagement Index in particular. After six straight years of decline, DHS FEVS scores went up three full percentage points, from 53% in 2015 to 56% this year. This is no anomaly and is regarded by the Office of Personnel Management as statistically significant. The results also compare favorably to the 1% increase across the entire Federal Government. In addition, the increased morale

2



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

at DHS was the largest increase of any Cabinet Department our size. Components will be integrating the new FEVS results into updated action plans that will be submitted in early 2017. A new DHS-wide action plan is in development as well. The action plan is based on employee feedback from the leadership town halls, the FEVS overall, and an agency-specific question on the FEVS.

Challenge #3: Acquisition Management

As the draft report notes, DHS “has instituted major reforms to the acquisition process and has exerted significant leadership to gain control of an unruly and wasteful process.” For example, major programs (Level 1 and 2) can no longer move to the next phase of the acquisition process without approved acquisition documentation. Given the significant improvements made in the areas of acquisition oversight and policy compliance and the ability to understand the cost, schedule, and performance parameters for these programs, DHS is now also applying lessons learned to non-major (Level 3) programs.

In 2015, DHS launched the Acquisition Innovations in Motion, a series of initiatives to improve communications with industry, ensure the continual improvement of business processes, and identify innovative approaches to conducting DHS procurements. In addition, DHS also institutionalized a staffing model that is now used by Component Acquisition Executives to develop staffing plans. The staffing plans identify staffing gaps and mitigation strategies to close identified gaps, which leadership monitors quarterly. Acquisition Review Boards (ARBs) review program staffing as well, to ensure this progress is sustained. When shortfalls are identified, “deep dive” reviews are conducted and recommendations made for structuring the program and mitigating critical gaps. The Acquisition Program Health Assessment was also implemented to provide early identification of critical issues within major acquisition programs. This tool is used to support monthly major acquisition program review meetings with all ARB members.

Challenge #4: Grants Management

As the draft report notes, “FEMA generally responded effectively to disasters,” ... but, “has not managed recovery from disasters well.” It is important to also note that in FY 2016, FEMA completed a multiyear initiative to redesign the process by which it provides Public Assistance (PA) and is now implementing a new PA delivery model. The model will improve the assessment of the damage to public infrastructure, streamline and ensure the consistent application of program policy and grant requirements, and help communities recover faster following a disaster. Throughout FY 2016, FEMA’s Grants Program Directorate has focused on its efforts to enhance grant oversight through the implementation of risk-based monitoring, verification of corrective actions for audit findings, draw down monitoring, and verifying compliance with grant requirements. Coupled with FEMA’s ongoing multiyear Grants Management Modernization program to coordinate business approaches for more than 40 different grants and develop a single



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Information Technology platform to integrate active grant programs and unify grants management life cycles and processes, these efforts are part of the Agency's long term, comprehensive solution to address root cause problems revealed through recurring OIG recommendations. This unified capability will address deficiencies FEMA has identified in its internal controls for existing grants management and administration processes and methods.

Challenge #5: Cybersecurity

As the draft report notes, OIG has found "incremental DHS progress in establishing an enterprise-wide information security program." DHS continues to work towards ensuring the security of federal information systems, critical infrastructure, and protecting the privacy of personally identifiable information. In addition, DHS is leading the Federal Government's efforts to improve civilian cybersecurity. This effort requires a whole-of-government approach and robust collaboration with the private sector. At the same time, DHS is improving its capability to develop and share situational awareness of cyber threats and vulnerabilities while providing a baseline of security for federal civilian agencies. In addition, DHS Senior Leadership proactively conducts quarterly meetings with Component Senior Leadership to discuss the Component's status in achieving FISMA compliance targets.

During the next year, DHS expects to make important progress reinforcing DHS's role in protecting the Federal Government's information systems and the Nation's critical infrastructure. Today, 80% of our federal civilian networks have adopted EINSTEIN 3 Accelerated and we are working to get all large federal departments and agencies on board by December 30, 2016. In addition, we will continue to work with civilian Federal Government agencies to procure and deploy Continuous Diagnostics and Mitigation Phase 2 capabilities, as well as expand participation in the Enhanced Cybersecurity Services Program. Finally, DHS will continue to expand the use of Cyber Security Advisors to assist private sector and state, local, tribal, and territorial government organizations in making improvements to their cybersecurity while providing them with access to other DHS cybersecurity resources.

Challenge #6: Management Fundamentals

As noted in the draft report, "The Department has made strides in establishing its management fundamentals, including obtaining an unmodified opinion on its financial statements for the last 3 years." DHS is taking a Unity of Effort approach to sustaining its management fundamentals and improving those categories identified by OIG.

Collecting the Right Data. One of the pillars of the Unity of Effort initiative is to strengthen DHS budget and acquisition processes. To this end, DHS developed the Common Appropriations Structure (CAS), a budget framework that enables strategic and

4



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

managerial decision making and comparability, and that clearly aligns expenses to the programs supported. As of October 1, 2016, DHS transitioned to the CAS. This new budgeting approach provides a simplified, consistent structure that allows the Department to compare like missions and activities. For example, DHS went from over 70 different appropriation types down to four common appropriations for all components. DHS has also begun to develop the “Planning, Programming, Budgeting, and Execution (PPBE) One-Number System.” When fully operational in FY 2019-2020, and in conjunction with Component financial system upgrades, the One-Number system will enhance DHS and component capability for complete, on-demand resource data for annual PPBE decisions. DHS has also begun its efforts to standardize data with the DHS Accounting Classification Structure, which is a key driver for business intelligence reporting. In addition, DHS has developed maturity models to assess the effectiveness of component internal controls (financial reporting controls and information systems controls). These models use a standard set of objectives to assess risks and controls across each component; the outcomes help management prioritize remediation requirements and assign resources.

Collecting and Analyzing Cost Data. DHS recognizes the importance of accurate, timely cost data as a key component for resource allocation, and is taking steps to establish a process for routinely collecting and analyzing cost data to inform decisions regarding our major acquisitions. For example, efforts to modernize DHS financial systems provide an opportunity to put mechanisms in place to track financial execution data by major acquisition program. Moreover, as DHS matures in acquisition and financial management, we are improving our ability to integrate the purpose and use of the life cycle cost estimate (LCCE) as a program management tool. In the past year, DHS also established the training cost working group, which has developed a methodology whereby Components will be able to track and record all costs associated with training. This data will be aggregated at the Department level to provide a true picture of the resources devoted to training DHS personnel.

Performance Measurement. DHS has a robust framework and guidance for establishing performance measures to communicate the results delivered to stakeholders associated with our DHS Strategic Plan. OIG’s specific references to TSA’s Screening of Passengers by Observation Techniques and CBP’s Streamline initiatives do not reflect the set of measures gauging our effectiveness to prevent terrorist attacks through a variety of passenger and baggage screening and vetting processes, nor the collection of measures to inform status of controlling the border.

The Department strives to continually improve gauging its effectiveness in a mission space difficult to quantify due to the nature of prevention and deterrence activities. We have a documented annual process to enhance the breadth and scope of our publically reported measure set, which is fully vetted and approved by the Office of Management and Budget. Furthermore, the Government Accountability Office, in the fall of 2015,

5



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

cited DHS as a best practice for our methods to ensure complete and reliable information is reported to the public on our set of over 80 measures known as our strategic or Government Performance and Results Act Modernization Act measures.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief 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
Chief Financial Officer
Chief Information Officer
Chief Security Officer
Chief Privacy Officer

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