# Roundtable on Reauthorizing the Department of Homeland Security

**Statement of George A. Scott, Managing Director, Homeland Security and Justice**

## Introduction

In the 15 years since the Department of Homeland Security's (DHS) creation, the department has implemented key homeland security operations, achieved important goals and milestones, and grown to more than 240,000 employees and over $65 billion in budget authority. We have issued hundreds of reports addressing the range of DHS's missions and management functions. Our work has identified gaps and weaknesses in the department's operational and implementation efforts, as well as opportunities to strengthen its efficiency and effectiveness. Since 2003, we have made approximately 2,700 recommendations to DHS to strengthen program management, performance measurement efforts, and management processes, among other things. DHS has implemented about 74 percent of these recommendations and has actions under way to address others.

We also report regularly to Congress on government operations that we 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, we designated *Implementing and Transforming DHS* as high-risk because DHS had to transform 22 agencies—several with major management challenges—into one department, and failure to address associated risks could have serious consequences for U.S. national and economic security.[1] Given the significant effort required to build and integrate a department as large and complex as DHS, our original high-risk designation addressed the department's initial transformation and subsequent implementation efforts, to include associated management and programmatic challenges.

Since 2003, the focus of the *Implementing and Transforming DHS* high-risk area has evolved in tandem with DHS's maturation and evolution. In our 2013 high-risk update, we reported that although challenges remained for DHS across its range of missions, the department had made considerable progress in transforming its original component agencies into a single cabinet-level department and positioning itself to achieve its full potential.[2] As a result, we narrowed the scope of the high-risk area to focus on strengthening DHS management functions (human capital, acquisition, financial management, and information technology (IT)) and changed the name of the high risk area to *Strengthening DHS Management Functions* to reflect this focus.

DHS also has critical responsibility in the high-risk area of *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information*. Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential

[1]GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

[2]GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: February 2013).

information.[3] The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. However, safeguarding federal computer systems and the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—has been a long-standing concern. In 1997, we designated federal information security as a government-wide high-risk area; we then expanded this high-risk area to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of personally identifiable information (PII) in 2015.[4] DHS is responsible for securing its own information systems and data and also plays a pivotal role in government-wide cybersecurity efforts.

Congress has been instrumental in supporting progress in individual high-risk areas and has also taken actions to pass various laws that, if implemented effectively, will help foster progress on high-risk issues. The Senate Committee on Homeland Security and Governmental Affairs' consideration of DHS reauthorization presents an important opportunity to establish mechanisms that can help further strengthen DHS management functions and information security efforts.

**2017 High-Risk Update Findings**

Our criteria for removing areas from the High-Risk List guide our advice to DHS and our assessment of its progress.[5] Specifically, it must have (1) a demonstrated strong commitment and top leadership support to address the risks; (2) the capacity (that is, the people and other resources) to resolve the risks; (3) a corrective action plan that identifies the root causes, identifies effective solutions, and provides for substantially completing corrective measures in the near term, including but not limited to steps necessary to implement solutions we recommended; (4) a program instituted to monitor and independently validate the effectiveness and sustainability of corrective measures; and (5) the ability to demonstrate progress in implementing corrective measures.

In our 2017 high-risk update, we reported on DHS's progress and work remaining in the *Strengthening DHS Management Functions* and *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information* high-risk areas.[6] We found that DHS had made progress in both areas, but that more work remains to strengthen management functions and the security over computer systems supporting federal operations and our nation's critical infrastructure.

In particular, we reported that DHS's continued efforts to strengthen and integrate its acquisition, IT, financial, and human capital management functions had resulted in the department meeting three

[3]Critical infrastructure includes systems and assets so vital to the United States that incapacitating or destroying them would have a debilitating effect on national security. These critical infrastructures are grouped by the following 16 industries or "sectors": chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology (IT); nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[4]GAO, *High-Risk List: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[5]GAO, *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: November 2000).

[6]GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

criteria for removal from the High-Risk List (leadership commitment, a corrective action plan, and a framework to monitor progress) and partially meeting the remaining two criteria (capacity and demonstrated, sustained progress), as shown in table 1.

**Table 1: GAO Assessment of Department of Homeland Security (DHS) Progress in Addressing the *Strengthening DHS Management Functions* High-Risk Area, as of February 2017**

| Criterion for removal from high-risk list | Met[a] | Partially met[b] | Not met[c] |
|---|---|---|---|
| Leadership commitment | X | | |
| Capacity | | X | |
| Action plan | X | | |
| Framework to monitor progress | X | | |
| Demonstrated, sustained progress | | X | |
| **Total** | **3** | **2** | **0** |

Source: GAO analysis of DHS documents, interviews, and prior GAO reports. | GAO-17-409T

[a]"Met": There are no significant actions that need to be taken to further address this criterion.

[b]"Partially met": Some but not all actions necessary to generally meet the criterion have been taken.

[c]"Not met": Few, if any, actions toward meeting the criterion have been taken.

DHS's top leadership, including the Secretary and Deputy Secretary of Homeland Security, demonstrated exemplary commitment and support for addressing the department's management challenges. For instance, the department's Deputy Secretary, Under Secretary for Management, and other senior management officials frequently met with us to discuss the department's plans and progress, which serves as a model for senior level engagement and helps ensure a common understanding of the remaining work needed to address our high-risk designation. Further, DHS established a framework for monitoring its progress in its *Integrated Strategy for High Risk Management*, in which it has included performance measures to track the implementation of key management initiatives since June 2012. In addition, since our 2015 high-risk update, DHS had strengthened its monitoring efforts for financial systems modernization programs that are key to effectively supporting the department's financial management operations, resulting in DHS meeting the monitoring criterion for the first time.

In our 2017 high-risk update we found that DHS had also issued updated versions of its *Integrated Strategy for High Risk Management,* demonstrating a continued focus on addressing this high-risk designation, and made important progress in identifying and putting in place the people and resources needed to resolve departmental management risks. The integrated strategy includes key management initiatives and related corrective action plans for achieving 30 outcomes, which we identified and DHS agreed are critical to addressing the challenges within the department's management areas, and to integrating those functions across the department. In our 2017 high-risk report, we found that DHS had fully addressed 13 of these outcomes, mostly addressed 8, partially addressed 6, and initiated the remaining 3, as shown in Table 2.

**Table 2: GAO Assessment of Department of Homeland Security (DHS) Progress in Addressing Key Outcomes, as of February 2017**

| Key management function | Fully addressed[a] | Mostly addressed[b] | Partially addressed[c] | Initiated[d] | Total |
|---|---|---|---|---|---|
| Acquisition management | 2 | 2 | 1 | | **5** |
| Information technology management | 3 | 3 | | | **6** |
| Financial management | 2 | | 3 | 3 | **8** |
| Human capital management | 3 | 3 | 1 | | **7** |
| Management integration | 3 | | 1 | | **4** |
| **Total** | **13** | **8** | **6** | **3** | **30** |

Source: GAO analysis of DHS documents, interviews, and prior GAO reports. | GAO-17-317

[a]"Fully addressed": Outcome is fully addressed.

[b]"Mostly addressed": Progress is significant and a small amount of work remains.

[c]"Partially addressed": Progress is measurable, but significant work remains.

[d]"Initiated": Activities have been initiated to address the outcome, but it is too early to report progress.

Of the 13 outcomes DHS had fully addressed, the department had sustained 9 as fully implemented for at least 2 years. For example, DHS had fully addressed one outcome for the first time by demonstrating improvement in human capital management by linking workforce planning efforts to strategic and program planning efforts. DHS also sustained full implementation of two other outcomes by obtaining a clean audit opinion on its financial statements for 4 consecutive fiscal years. However, we reported that considerable work remained in several areas for DHS to fully achieve the remaining 17 outcomes and thereby strengthen its management functions. In particular, we found that addressing some of these outcomes, such as those pertaining to improving employee morale and modernizing the department's financial management systems, are significant undertakings that will likely require multiyear efforts.

Additionally, we reported that DHS needed to make additional progress identifying and allocating resources in certain areas—including financial systems modernization projects and acquisition and IT staffing—to sufficiently demonstrate that it had the capacity (that is, the people and resources) to achieve and sustain all 30 outcomes.

In regard to the *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information* high-risk area, we found in our 2017 high-risk update that:

- The Executive Office of the President (EOP) and DHS met the criterion of demonstrating top leadership commitment. Specifically, DHS established the Critical Infrastructure Cyber Community (C3) Voluntary Program to encourage entities to adopt the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.[7] As part of this program, DHS developed guidance and tools that were intended to help entities use the framework. The C3 Voluntary Program also included outreach and awareness activities, promotion of efforts targeting specific types of entities, and creation of communities of interest around critical infrastructure cybersecurity.

[7]NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014).

- The EOP, DHS, and federal agencies partially met the criterion for implementing programs to monitor corrective actions related to cybersecurity and PII protection. Specifically, the EOP and DHS developed and used metrics for measuring agency progress in implementing initiatives on information security regarding continuous monitoring, strong authentication, and anti-phishing and malware defense. In addition, the Office of Management and Budget (OMB) and DHS continued to monitor agencies' implementation of information security requirements using Federal Information Security Modernization Act reporting metrics.

- The EOP, DHS, and federal agencies partially met the criterion to demonstrate progress in implementing the many requirements for securing federal systems and networks. For example, OMB and DHS conducted CyberStat reviews at federal agencies during fiscal years 2015 and 2016.[8] Nevertheless, we reported that federal agencies needed to consistently demonstrate progress. Specifically, for DHS, in January 2016, we reported that DHS's National Cybersecurity Protection System[9] was partially, but not fully, meeting its stated system objectives of detecting intrusions, preventing intrusions, analyzing malicious content, and sharing information.[10] DHS also had not developed metrics for measuring the performance of the system. In addition, we reported in December 2015 that while DHS established the C3 Voluntary Program to encourage entities to adopt NIST's *Framework for Improving Critical Infrastructure Cybersecurity* in the critical infrastructure sectors, it had not developed metrics to measure the success of its activities and programs.[11]

**Updates from Subsequent GAO Monitoring and Reports**

Since our February 2017 high-risk update we have continued to monitor and report on DHS's efforts to resolve the risks presented by the *Strengthening DHS Management Functions* and *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information* high-risk areas.

With respect to the *Strengthening DHS Management Functions* high-risk area, DHS continues to meet three and partially meet two criteria for removal from the High-Risk List. In particular:

- DHS continues to meet the leadership commitment, corrective action plan, and framework to monitor progress criteria. For example, DHS submitted two additional *Integrated Strategy for*

[8]CyberStat reviews are in-depth sessions with national security staff, OMB, DHS, and an agency to discuss that agency's cybersecurity posture and discuss opportunities for collaboration.

[9]The National Cybersecurity Protection System, operationally known as the EINSTEIN program, is an integrated system-of-systems that is intended to deliver a range of capabilities, including intrusion detection, intrusion prevention, analytics, and information sharing.

[10]GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

[11]We further reported in our 2017 High-Risk update that the EOP, DHS, and federal agencies partially met the capacity and corrective action plan criteria. Our findings focused primarily on EOP and OMB actions and not DHS actions.

*High-Risk Management* updates—one for March 2017 and one for September 2017—which we assessed and provided feedback on to DHS senior leadership.[12]

- DHS continues to partially meet the capacity criterion. Specifically, DHS has continued its efforts to identify and allocate resources for financial systems modernization projects and acquisition and IT staffing, but additional progress is needed to fully identify the people and other resources needed in these areas. For example, in our 2017 high-risk update we reported that DHS planned to shift its IT paradigm from acquiring assets to acquiring services and acting as a service broker. While DHS had issued a workforce planning contract to help the department transition to the skillsets needed to accommodate the service broker model, department officials had not yet defined what those skill sets were or analyzed the skills gaps resulting from the paradigm shift.

  In May 2017, we recommended that DHS establish time frames and implement a plan for (1) identifying the department's future IT skillset, (2) conducting a skills gap analysis, and (3) resolving any skills gaps identified.[13] DHS concurred and reported efforts underway to implement this recommendation. However, until DHS completes these steps, the department's capacity to support the paradigm shift remains unclear.

- Further, DHS continues to partially meet the demonstrated, sustained progress criterion. Since our 2017 high-risk update, DHS's efforts to achieve the 17 outcomes it had not fully addressed have resulted in the department fully addressing an additional human capital management outcome by demonstrating that DHS components are basing hiring decisions and promotions on human capital competencies.

  Conversely, DHS has not fully sustained its efforts related to an IT management outcome focusing on investment management. We reported that DHS had fully addressed this outcome for the first time in our 2015 high-risk update as a result of DHS annually reviewing each of its functional portfolios of investments across the entire department, to determine the most efficient allocation of resources within each of the portfolios. However, according to DHS officials, for the past two fiscal years (during the development of the fiscal year 2018 and 2019 budgets), DHS reviewed its investments by portfolio only within a component, and not across all components. As a result, the department's ability to identify potentially duplicative investments and opportunities for consolidating investments across the entire department may be limited. DHS officials plan to provide evidence of other efforts they believe meet the intent of the outcome, which we will assess upon receipt.

[12]The National Defense Authorization Act for Fiscal Year 2017 includes a provision for the DHS Under Secretary for Management to report to us every 6 months to demonstrate measurable, sustainable progress made in implementing DHS's corrective action plans to address the *Strengthening DHS Management Functions* high-risk area until we submit written notification of the area's removal from the high-risk list to the appropriate congressional committees. See Pub. L. No. 114-328, § 1903(b), 130 Stat. 2000, 2673 (2016) (classified at 6 U.S.C. § 341(a)(11)).

[13]GAO, *Homeland Security: Progress Made to Implement IT Reform, but Additional Chief Information Officer Involvement Needed,* GAO-17-284 (Washington, D.C.: May 18, 2017).

Although DHS's mostly and partially addressed ratings for the remaining outcomes have not changed, the department continues to make progress toward achieving them. For example, in October 2016, DHS established the Acquisition Program Health Assessment, a process intended to monitor major acquisition programs' progress. The assessment methodology—which DHS is in the process of implementing—consists of a number of factors, such as program management, financial management, and contract management, which DHS deemed were important for successful program execution.

Additionally, DHS has continued to strengthen its employee engagement efforts by implementing our September 2012 recommendation to establish metrics of success within action plans the department developed for addressing its employee satisfaction problems.[14] Further, the Office of Personnel Management's 2017 Federal Employee Viewpoint Survey data showed that DHS's scores increased in four areas (leadership and knowledge management, results-oriented performance culture, talent management, and job satisfaction) for the second year in a row; a considerable improvement over the department's scores generally declining from 2008 through 2015.

Nonetheless, significant work remains in certain areas. For example in May 2017, we reported on DHS implementation of Federal Information Technology Acquisition Reform Act (FITARA) provisions.[15] We found that DHS faces challenges in implementing certain FITARA provisions—including Chief Information Officer (CIO) approval of contracts and agreements and CIO evaluation of risk—and concluded that until DHS addresses these challenges, the goal of FITARA to elevate the role of the department CIO in acquisition management will not be fully realized. Additionally, in September 2017 we reported that better use of best practices, such as those for managing project risks, could help DHS manage financial systems modernization projects that are key to effectively supporting the department's financial management operations.[16]

In regard to the *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information* high-risk area:

- In February 2017, we reported on DHS's National Cybersecurity and Communications Integration Center (NCCIC), which is to provide a central place for the various federal and private-sector organizations to coordinate efforts to address and respond to cyber threats.[17] We found that DHS had taken steps to perform each of its 11 statutorily required cybersecurity

[14]GAO, *Department of Homeland Security: Taking Further Action to Better Determine Causes of Morale Problems Would Assist in Targeting Action Plans*, GAO-12-940 (Washington, D.C.: Sept. 28, 2012).

[15]GAO-17-284; Pub. L. No. 113-291, tit. VIII, subtit. D, 128 Stat. 3292, 3438-50 (2014).

[16]GAO, *DHS Financial Management: Better Use of Best Practices Could Help Manage System Modernization Project Risks,* GAO-17-799 (Washington, D.C.: Sep. 26, 2017).

[17]GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely,* GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

functions.[18] However, the extent to which the center performed its functions in accordance with nine implementing principles established in the law was unclear because the center had not determined the applicability of the principles to all 11 functions or established metrics and methods by which to evaluate its performance against the principles. [19] While in some instances NCCIC had implemented functions in accordance with one or more of the principles, in others this was not the case. 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.

In addition, several factors impeded 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 because they did not have access to all relevant data, limiting the center's 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. We recommended nine actions for enhancing the effectiveness and efficiency of NCCIC, including determining the applicability of the implementing principles and establishing metrics and methods for evaluating performance; and addressing identified impediments. DHS concurred with our recommendations and continues to take action to address them.

- In September 2017, we reported that DHS, in its role under the Federal Information Security Modernization Act of 2014, issued cybersecurity-related directives and continued to monitor cybersecurity incidents.[20] In particular, DHS developed several binding operational directives that were intended to address critical cyber vulnerabilities and cyber incidents. Also, DHS provided security capabilities for agencies to enhance the detection of cyber vulnerabilities and protect against cyber threats through the National Cybersecurity Protection System and the continuous diagnostic and mitigation program.

- Currently, we are assessing what is known about the extent to which 16 critical infrastructure sectors established in federal policy, including 10 sectors for which DHS serves as the lead agency, have adopted the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*.[21] Additionally, we have ongoing work to examine

[18]NCCIC functions identified in the National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066, and the Cybersecurity Act of 2015, Pub. L. No. 114-113, div. N, 129 Stat. 2242, 2935-85, include, among others, (1) being a federal civilian interface for sharing cybersecurity-related information with federal and nonfederal entities; (2) providing shared situational awareness to enable real-time, integrated, and operational actions across the federal government and nonfederal entities to address cybersecurity risks and incidents to federal and nonfederal entities; and (3) coordinating the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks and incidents across the federal government.

[19]NCCIC principles identified in the National Cybersecurity Protection Act of 2014 include, among others, (1) ensuring that timely, actionable, and relevant information related to risks, incidents, and analysis is shared and (2) ensuring that when appropriate, information related to risks, incidents, and analysis is integrated with other information and tailored to a sector. Pub. L. No. 113-282, 128 Stat. 3066.

[20]GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017); Pub. L. No. 113-283, 128 Stat. 3073 (2014).

[21]*Presidential Policy Directive-21—Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

the extent to which DHS has identified, categorized and assigned employment codes to its cybersecurity positions; and identified its cybersecurity workforce areas of critical need as required by the Homeland Security Cybersecurity Workforce Assessment Act.[22] We plan to issue our reports for both of these reviews later this month.

**Priority Issues for Consideration as Part of DHS Reauthorization**

While DHS has made some progress in addressing key issues, the reauthorization of DHS provides an important opportunity to address longstanding issues and better position the department to more efficiently and effectively carry out its mission. The following are some of the highest priority issues to be addressed and specific corrective actions GAO has called for DHS to implement across a range of management and mission areas. The reauthorization bill under consideration could be used to codify or otherwise address these issues.

Acquisition Management

- DHS should require that major acquisition programs' technical requirements are well defined and key technical reviews are conducted prior to approving programs to initiate product development and establishing acquisition program baselines, in accordance with acquisition best practices. In addition, DHS should specify that acquisition decision memorandums clearly document the rationale of decisions made by DHS leadership, such as, but not limited to, the reasons for allowing programs to deviate from the requirement to obtain department approval for certain documents at Acquisition Decision Events and the results of considerations or trade-offs. Further, DHS should specify at what point minimum standards for key performance parameters should be met, and clarify the performance data that should be used to assess whether or not a performance breach has occurred. (GAO-17-346SP)

- DHS should establish a time frame for components to identify all of their non-major acquisitions. (GAO-17-396)

- DHS should enhance its leadership's ongoing efforts to improve the affordability of the department's major acquisitions portfolio by ensuring that Future Years Homeland Security Program reports reflect the results of any tradeoffs stemming from the acquisition affordability reviews; and require components to establish formal, repeatable processes for addressing major acquisition affordability issues. (GAO-16-338SP)

- DHS should ensure consistent, effective oversight of DHS's acquisition programs and make the Comprehensive Acquisition Status Report (CASR) more useful by adjusting the CASR to report an individual rating for each program's cost, schedule, and technical risks, and the level at which the program's life-cycle cost estimate was approved. (GAO-15-292)

[22]The Homeland Security Cybersecurity Workforce Assessment Act was enacted as part of the Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277 § 4,128 Stat. 2995, 3008-10 (2014) (6 U.S.C. § 146 note).

- DHS should ensure the U.S. Coast Guard acquisition funding plans presented to Congress are comprehensive and clearly account for all operations and maintenance funding DHS plans to allocate to each of the programs. (GAO-15-171SP)

Information Technology Management and Cybersecurity

- DHS should ensure that it fully and effectively implements FITARA by, among other things, addressing challenges related to Chief Information Officer contract approval and evaluation of risks associated with the department's IT investments. (GAO-17-284)

- DHS's Chief Information Officer should use accurate and reliable information, such as operational assessments of the new architecture and cost and schedule parameters approved by the Under Secretary of Management, to help ensure that assessments prepared by the Office of the Chief Information Officer in support of the department's updates to the federal IT Dashboard more fully reflect the current status of the Transformation Program. (GAO-15-415)

- DHS needs to remediate the material weakness in information security controls reported by its financial statement auditor in fiscal year 2017 by effectively addressing weaknesses in controls related to access, configuration management, and segregation of duties.[23]

- DHS should ensure that its Human Resources IT (HRIT) program receives necessary oversight and attention by: (1) updating and maintaining a schedule estimate for when DHS plans to implement each of the strategic improvement opportunities; (2) developing a complete life-cycle cost estimate for the implementation of HRIT; and (3) documenting and tracking all costs, including components' costs, associated with HRIT. (GAO-16-253)

Human Capital Management

- DHS needs to continue to address employee morale problems through comprehensively examining root causes within DHS and its components' action plans**.** (GAO-12-940)

Financial Management

- DHS should develop and implement effective processes and improve guidance to reasonably assure that future alternative analyses for financial systems initiatives fully follow analysis of alternatives (AOA) process best practices and reflect the four characteristics of a reliable, high-quality AOA process. (GAO-17-799)

- DHS should improve the *Risk Management Planning Handbook* and other relevant guidance for managing risks associated with financial management system modernization projects to fully incorporate risk management best practices. (GAO-17-799)

- DHS needs to put in place sound internal controls and financial reporting systems to address its long-term challenges in sustaining a clean audit opinion on its financial statements and in

[23]DHS, Independent Auditors' Report on DHS' FY 2017 Financial Statements and Internal Control over Financial Reporting, OIG-18-16 (Washington, D.C.: November 2017).

obtaining and sustaining a clean opinion on its internal controls over financial reporting. This is needed to ensure that the department's financial management systems generate reliable, useful, and timely information for day-to-day decision making as a routine business operation.

Emergency Preparedness and Response

- Federal Emergency Management Agency (FEMA) should develop a methodology to better assess a jurisdiction's capability to respond to and recover from a disaster without federal assistance. This should include one or more measures of a jurisdiction's fiscal capacity, such as Total Taxable Resources, and consideration of the jurisdiction's response and recovery capabilities. If FEMA continues to use the Public Assistance per capita indicator to assist in identifying a jurisdiction's capabilities to respond to and recover from a disaster, it should adjust the indicator to accurately reflect the annual changes in the U.S. economy since 1986, when the current indicator was first adopted for use. In addition, implementing the adjustment by raising the indicator in steps over several years would give jurisdictions more time to plan for and adjust to the change. (GAO-12-838)

Border Security

- U.S. Customs and Border Protection should assess the effectiveness of deployed technology systems. (GAO-14-368)

- U.S. Citizenship and Immigration Services should (1) conduct regular fraud risk assessments across the affirmative asylum application process and (2) identify and implement tools that asylum officers and Fraud Detection and National Security Directorate immigration officers can use to detect potential fraud patterns across affirmative asylum applications. (GAO-16-50)

- Border Patrol should (1) develop metrics to assess the contributions of pedestrian and vehicle fencing to border security along the southwest border and (2) develop and implement written guidance to include roles and responsibilities for the steps within its requirements process for identifying, funding, and deploying tactical infrastructure assets for border security operations. (GAO-17-331)

Transportation Security

- DHS should limit funding for the Transportation Security Administration's (TSA) behavior detection activities until TSA provides scientifically valid evidence of their effectiveness. (GAO-14-159)

- DHS, through TSA and the U.S. Coast Guard's combined efforts, should conduct an assessment of the Transportation Worker Identification Credential Program's effectiveness to determine whether the benefits of continuing to implement and operate the program in its present form and planned use with readers surpass the costs. (GAO-11-657)

Infrastructure

- Before requesting additional funding for the DHS headquarters consolidation project, DHS and the General Services Administration (GSA) should conduct (1) a comprehensive needs assessment and gap analysis of current and needed capabilities that take into consideration changing conditions, and (2) an alternatives analysis that identifies the costs and benefits of leasing and construction alternatives for the remainder of the project and prioritizes options to account for funding instability. (GAO-14-648)

- DHS and GSA should develop revised cost and schedule estimates for the remaining portions of the consolidation project that conform to GSA guidance and leading practices for cost and schedule estimation, including an independent evaluation of the estimates. DHS should also designate the headquarters consolidation program a major acquisition, consistent with DHS acquisition policy, and apply DHS acquisition policy requirements. (GAO-14-648)