OFFICE OF INSPECTOR GENERAL

Testimony of Acting Inspector General John V. Kelly

Committee on Homeland Security and Governmental Affairs

United States Senate

"Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland"

Homeland Security

February 7, 2018
10:00 AM

Good morning Chairman Johnson, Ranking Member McCaskill, and Members of the Committee. Thank you for inviting me today to discuss the reauthorization of the Department of Homeland Security (DHS).

Since its establishment, DHS has progressed in addressing challenges to accomplish its mission. However, to fulfill its vital mission of protecting and securing our Nation successfully, the Department must continue to overcome challenges that hinder its efforts.

My testimony today will focus on the management and acquisition challenges the Department has faced, progress made in addressing these challenges, and potential reforms to address outstanding challenges. H.R. 2825, *The Department of Homeland Security Authorization Act of 2017* (DHS Authorization Act), serves to streamline oversight, communication, responsibility, and accountability of the Department's management and acquisition functions. By addressing these areas, DHS can continue to improve its operations and reduce waste, fraud, and abuse. However, if the Department ignores these outstanding challenges, it will be difficult for DHS to effectively and efficiently address new and emerging threats to the homeland.

Priorities and Challenges

DHS faces many long-standing challenges, and we at the Office of Inspector General (OIG) have focused our energy on the Department's major management and performance challenges. The challenges are two-fold. First, Department leadership must commit itself to ensuring DHS operates more as a single entity rather than a collection of components. The lack of progress in reinforcing a unity of effort translates to a missed opportunity for greater effectiveness.

Second, Department leadership must establish and enforce a strong internal control environment typical of a more mature organization. The current environment of relatively weak internal controls affects all aspects of the Department's mission, from border protection to immigration enforcement and from protection against terrorist attacks and natural disasters to cybersecurity.[1]

Challenges in Committing to Intra-component Cooperation

In the last few years, the Department has formally attempted to establish a centralized authority structure through its "One DHS" and "Unity of Effort" initiatives. These initiatives have largely been executed through DHS Management Directives on budget formulation and acquisition activities, as

[1] *Major Management and Performance Challenges Facing the Department of Homeland Security*, OIG-18-11 (November 2017).

well as high-level coordination activities often spearheaded by senior Department leadership. Unity of Effort appears to be ongoing, but the Department will continue to be challenged to sustain and implement such initiatives as the Department's mission continues to evolve.

Fortunately, the DHS Authorization Act will further reinforce the Department's unity by streamlining the oversight, communication, responsibility, and accountability of its programs and offices, thereby eliminating the redundancy and overlap that makes a unified organization impossible.

The central challenge of a young DHS is to forge a number of disparate entities, each with a unique culture, history, and mission focus into a single entity. This requires senior-level, proactive communication and strong internal controls; to do otherwise risks the perception of a tacit message that the components can simply consider the Department an umbrella organization and continue to go it alone.

Our previous audit and inspection reports are replete with examples of the consequences of failing to act as a single entity:

- Our 2013 audit of DHS' H-60 helicopter programs showed that components did not cooperate with another to realize potential cost savings and other efficiencies. Specifically, CBP was unwilling to coordinate with the Coast Guard to upgrade its H-60 helicopters, even though both components were converting the same helicopters. We estimated potential savings of about $126 million if the two components had successfully coordinated the conversion of CBP's H-60 helicopters at the Coast Guard's Aviation Logistics Center. A subsequent H-60 Business Case Analysis by DHS' Office of Chief Readiness Support Officer, the Aviation Governing Board, the Coast Guard, and CBP confirmed the cost savings of having the Coast Guard convert the helicopters, but it was too late.[2]

- DHS employs approximately 80,000 Federal law enforcement officers whose positions allow for the use of force as they perform their duties; however, DHS does not have an office responsible for managing and overseeing component use-of-force activities. We discovered that each component varies on its use-of-force activities and DHS has no centralized oversight of use-of-force allegations, trends, training, facilities, and resource challenges faced by field personnel. We recently recommended that DHS establish a

[2] *DHS' H-60 Helicopter Programs (Revised)*, OIG-13-89 (May 2013).

department-level entity to actively oversee and assist with component use-of-force activities, update policies, and improve training.[3]

- Since its formation, DHS has faced challenges in integrating various component training facilities and programs, and does not have adequate oversight of its workforce training. Multiple prior audits have shown DHS does not have reliable training cost data and information to make informed management decisions. During our 2016 audit, we attempted to determine total DHS training costs for FYs 2014 and 2015. When we requested DHS training costs from the DHS Office of the Chief Financial Officer (OCFO), it could not readily provide the data. The OCFO did not have access to components' financial systems; rather, it relied on data calls to provide the training costs and could not validate the data. As a result, we found significant discrepancies between the total amounts reported by DHS. Although DHS has taken steps to improve the reliability of its training data, further action is needed—thus, we recommended that the Under Secretary for Management develop and implement a process to accurately capture and report training information across DHS.[4]

We believe the DHS Authorization Act is an important step toward the structural changes that are needed to create a unified Department.

Acquisition Management

While the Department has made progress in addressing the challenges it faces in major and non-major acquisitions and program management, it continues to face challenges in these areas. Acquisition management, which is critical to fulfilling all DHS missions, is inherently complex and high risk. It is further challenged by the magnitude and diversity of the Department's procurements. 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 financial, human resource, and information technology (IT) systems. DHS' yearly spending on contractual services and supplies, along with acquisition of assets, exceeds $33 billion.[5] Although the Department has improved its acquisition processes and taken steps to strengthen oversight of major acquisition programs, challenges to cost effectiveness and efficiency remain.

---

[3] *DHS Lacks Oversight of Component use of Force*, OIG-17-22 (January 2017).
[4] *DHS' Oversight of Its Workforce Training Needs Improvement*, OIG-16-19 (January 2016).
[5] According to DHS' *FY 2017 Agency Financial Report*, the Department's FY 2017 expenditures for "Contractual Services and Supplies" were about $29.1 billion and its expenditures for "Acquisition of Assets" were about $4.2 billion.

Legislative Progress

In 2017, we communicated to the Committee our support for five bills under consideration by Congress: the *DHS Acquisition Review Board Act of 2017* (S. 886), the *DHS Multiyear Acquisition Strategy Act of 2017* (S. 887), the *DHS Acquisition Authorities Act of 2017* (S. 902), the *Reducing DHS Acquisition Cost Growth Act* (S. 906), and the bill to establish the Joint Requirements Council. These bills would institutionalize the significant reforms already made, and therefore, prevent backsliding into past poor performance; address some of the outstanding challenges; and allow room for additional improvements as the Department continues to build its acquisition management capabilities. These bills codify existing policy and relevant offices; provide the necessary authority for key personnel and mechanisms within the Department to more effectively identify needed capabilities and validate operational requirements, to better manage major acquisition programs; and reinforce the importance of key acquisition management practices, such as establishing cost, schedule, and performance parameters, as well as decision gates that identify and address poorly performing acquisition programs.

Likewise, the DHS Authorization Act would protect taxpayer dollars and hold DHS more accountable through reforms to DHS's acquisition processes to ensure billions of taxpayer dollars are better safeguarded and tools to secure the homeland are delivered efficiently. It would strengthen the role of the Under Secretary for Management to implement efficiencies across components to better ensure proper oversight and accountability.

Ongoing Challenges

Although DHS has made much progress, it has not yet achieved the cohesion and sense of community to act as one entity working toward a common goal. The Department needs to continue toward a strong central authority and uniform policies and procedures throughout the Department. While the policy and guidance have been revised at the Department level for Level 1 and 2 programs, Level 3 programs continue to have component level guidance. In February 2017, the Department issued the MD-102-01-010, Level 3 Acquisition Management. This guidance establishes DHS strategic governance for the Department's Level 3 acquisition program activities and consolidates Level 3 direction into a single instruction. While robust, this guidance applies only to those organizations that fall under the Under Secretary of Management. Components, such as CBP and Coast Guard, are free to establish their own Level 3 guidance.

Most of DHS' major acquisition programs continue to cost more than expected, take longer to deploy than planned, or deliver less capability than promised. Although its acquisition policy includes best practices, DHS sometimes approves moving forward with major acquisition programs without appropriate internal oversight.

- FEMA is unable to assess flood hazard miles to meet its program goal and is not ensuring mapping partner quality reviews are completed in accordance with applicable guidance. FEMA needs to improve its management and oversight of flood mapping projects to achieve or reassess its program goals and ensure the production of accurate and timely flood maps. Specifically, FEMA: needs to improve its financial management of flood map projects to achieve or to reassess its program goal of 80 percent New, Valid, or Updated Engineering program miles; has not updated its Risk MAP life cycle cost estimate to inform critical decision-making; lacks uniform, centralized policies and procedures for projects placed on hold; and is not performing adequate oversight to ensure mapping partner quality reviews comply with requirements set forth in applicable guidance. Without accurate floodplain identification and mapping processes, management, and oversight, FEMA cannot provide members of the public with a reliable rendering of their true flood vulnerability or ensure that National Flood Insurance Program rates reflect the real risk of flooding.[6]

- USCIS still uses a paper file system to process immigration benefits and spends $300 million per year just to store and transport its 20 million immigrant paper files. USCIS has been attempting to automate this process since 2005, but despite spending more than $500 million on the technology program between FYs 2008 and 2012, little progress has been made. Past automation attempts have been hampered by ineffective planning, multiple changes in direction, and inconsistent stakeholder involvement. USCIS deployed the Electronic Immigration System (ELIS) in May 2012, but at the time we issued our report, customers could 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.[7]

  These failures have a real impact on our national security. Because of processing errors resulting from premature release of ELIS software, USCIS

[6] *FEMA Needs to Improve Management of Its Flood Mapping Programs*, OIG-17-110 (September 2017).
[7] *USCIS Automation of Immigration Benefits Processing Remains Ineffective*, OIG-16-48 (March 2016).

received over 200,000 reports from approved applicants about missing green cards. The number of cards sent to wrong addresses has incrementally increased since 2013 due in part to complex processes for updating addresses, ELIS limitations, and factors beyond the agency's control. USCIS produced at least 19,000 cards that included incorrect information or were issued in duplicate. Most card issuance errors were due to design and functionality problems in ELIS. USCIS' efforts to address the errors have been inadequate. Although USCIS conducted a number of efforts to recover the inappropriately issued cards, these efforts also were not fully successful and lacked consistency and a sense of urgency. Errors can result in approved applicants unable to obtain benefits, maintain employment, or prove lawful immigration status. In the wrong hands, Green Cards may enable terrorists, criminals, and illegal aliens to remain in the United States and access immigrant benefits.[8]

Finally, we issued a management alert as it related to the USCIS rollout of the N-400 form on ELIS in January of last year. The use of ELIS has impaired the ability of USCIS Immigration Services Officers and field personnel to conduct naturalization processing. In the course of our audit work, we discovered significant deficiencies in background and security checks for applicants, including 175 applicants who were granted citizenship with incomplete or inaccurate background checks. We are pleased to report that USCIS has agreed to delay the return to ELIS processing until all of the technical issues have been resolved.[9]

- DHS Performance and Learning Management System (PALMS) does not address the Department's critical need for an integrated, department-wide learning and performance management system. As of October 2016, PALMS had not met DHS operational requirements for effective administration of employee learning and performance management activities. This occurred because the PALMS program office did not effectively implement its acquisition methodology and did not monitor contractor performance. GAO also reported in its February 2016 report, GAO-16-253, that the Department experienced programmatic and technical challenges that led to years-long schedule delays. As a result, despite obligating $27.2 million as of December 2016, DHS PALMS does not achieve the intended benefits or address the Department's needs. In addition, between August 2013 and November 2016, the Department spent more than $5.7 million for unused

[8] *Better Safeguards are Needed in USCIS Green Card Issuance*, OIG-17-11 (November 2016)
[9] *Management Alert – U.S. Citizenship and Immigration Services' Use of the Electronic Immigration System for Naturalization Benefits Processing*, OIG-17-26-MA (January 2017)

and partially used subscriptions; $11 million to extend contracts of existing learning management systems, and $813,000 for increased program management costs. The Department also did not identify $72,902 in financial credits stemming from the contractor not meeting performance requirements between June and September 2015.[10]

Components not following guidance

Components do not always follow departmental acquisition guidance, which may lead to cost overruns, missed schedules, and mediocre acquisition performance. All of these have an effect on budget, security, and efficient use of resources.

- Although the United States Coast Guard approved approximately $ 1.8 billion of IT procurements between FY 2014 and 2016, it does not know if almost 400 information systems are receiving proper acquisition oversight. 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.

  Specifically: acquisition and IT review processes operate independent of each other, creating inefficiencies and weaknesses that can compromise the success of an IT acquisition program; there are insufficient controls to ensure that IT investments are reviewed to identify and designate the appropriate level of acquisition oversight; lack of reliable or non-existent information hinders efforts to determine that information systems may require additional acquisition oversight; and, the Coast Guard has not updated its acquisition and IT manuals, which currently provide insufficient guidance.

  These control weaknesses affect the Coast Guard's ability to effectively oversee non-major IT programs. Programs that to not receive adequate oversight are at risk of wasting money, missing milestones, and not achieving performance requirements. For instance, the Coast Guard spent approximately $68 million on the Integrated Health Information System in a failed attempt to modernize its electronic health records system.[11]

- CBP currently faces an aggressive implementation schedule to satisfy its requirements under the President's Executive Order. CBP is working on an

[10] *PALMS Does Not Address Department Needs*, OIG-17-91 (June 2017).
[11] *Coast Guard IT Investments Risk Failure Without Required Oversight*, OIG-18-15 (November 2017).

acquisition plan while simultaneously preparing a solicitation for the design and build of a southern border wall. CBP must continue to be mindful of the lessons learned related to an aggressively scheduled acquisition in order to protect taxpayer dollars associated with the acquisition of the construction of a southern border wall. Prior reports found that CBP did not have defined and validated operational requirements resulting in unachievable performance. CBP also lacked a proper acquisition workforce that resulted in missteps, waste, and delays. In addition, CBP did not have robust business processes and information systems needed to enable program offices to move forward expeditiously on the tasks of managing to program objectives.[12]

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

  The Department must take additional steps to improve IT investment transparency, risk management, and review and reporting processes in line with FITARA. The CIO office has implemented several key enhancements, such as updating the agency-wide IT portfolio review process. However, other requirements such as reporting on the use of incremental development and conducting program reviews of high-risk investments were not fully met. These shortfalls were due, in part, to incomplete departmental processes to ensure compliance. Until these requirements are fully implemented, DHS will be challenged to ensure accurate reporting on adoption of incremental development and timely reviews of its high-risk IT investments.[13]

- As described in our prior reports on this issue, numerous deficiencies continue in Security Technology Integrated Program (STIP) IT security

[12] *Special Report: Lessons Learned from Prior Reports on CBP's SBI and Acquisitions Related to Securing our Border*, OIG-17-70-SR (June 2017).
[13] *DHS' Progress in Implementing the Federal Information Technology Acquisition Reform Act*, OIG-16-138 (Revised) (October 2016).

controls, including unpatched software and inadequate contractor oversight. This occurred because TSA typically has not managed STIP equipment in compliance with departmental guidelines regarding sensitive IT systems. Failure to comply with these guidelines increases the risk that baggage screening equipment will not operate as intended, resulting in potential loss of confidentiality, integrity, and availability of TSA's automated explosive, passenger, and baggage screening programs.

TSA did not effectively manage all IT components of STIP as IT investments. Based on senior-level TSA guidance, TSA officials did not designate these assets as IT equipment. As such, TSA did not ensure that IT security requirements were included in STIP procurement contracts, which promoted the use of unsupported operating systems that created security concerns and forced TSA to disconnect STIP TSE from the network. TSA also did not report all STIP IT costs in its annual budgets, hindering the agency from effectively managing and evaluating the benefits and costs of STIP.[14]

Given the magnitude and risks of the Department's acquisitions, we will continue to evaluate this critical area. The urgency and complexity of DHS' mission will continue to demand rapid pursuit of major investment programs. As DHS continues to build its acquisition management capabilities, it will need stronger departmental oversight and authority, as well as increased commitment by the components to effect real and lasting change. This commitment includes adhering to departmental acquisition guidance, adequately defining requirements, developing performance measures before making new investments, and dedicating sufficient resources to contract oversight. All of this will better support DHS' missions and save taxpayer dollars.

Aviation Security

Nowhere is the asymmetric threat of terrorism more evident than in the area of aviation security. TSA cannot afford to miss a single, genuine threat without potentially catastrophic consequences, and yet a terrorist only needs to get it right once. The DHS Authorization Act will strengthen aviation security, which remains a formidable task – with TSA responsible for screening travelers and baggage for over 1.8 million passengers a day at 450 of our Nation's airports.

Detection of dangerous items on people and in baggage requires reliable equipment with effective technology, as well as well-trained and alert TSOs who

[14] *IT Management Challenges Continue in TSA's Security Technology Integrated Program (Redacted)*, OIG-16-87 (May 2016).

understand and consistently follow established procedures and exercise good judgment. We believe there are vulnerabilities in TSA's screening operations, caused by a combination of technology failures and human error. Since 2004, we have conducted nine covert penetration testing audits on passenger and baggage screening operations.

Previous covert testing identified vulnerabilities in TSA's use of Advanced Imaging Technology (AIT) equipment at domestic airports. We previously engaged in covert penetration testing to evaluate the effectiveness of TSA's Automated Target Recognition software and checkpoint screener performance in identifying and resolving potential security threats at airport checkpoints. The specific result of our covert testing, like the testing we have done in the past, is classified at the Secret level. However, we can describe the results as troubling and disappointing. [15]

Unfortunately, the results of this covert testing was in line with previous covert testing we had conducted, both on the AIT machines as well as on checked baggage and access to secured airport areas. [16]

I am pleased to report that that TSA's leadership understood the gravity of our findings, and moved to revamp training, improve technology, and refine checkpoint policies and procedures in an attempt to increase checkpoint effectiveness. This plan is appropriate because the checkpoint must be considered as a single system; the most effective technology is useless without the right personnel, and the personnel need to be guided by the appropriate procedures. Unless all three elements are operating effectively, the checkpoint will not be effective.

In 2017, we also audited the Federal Air Marshal Service's (FAMS) contribution to TSA's layered approach to security. Although our results are classified or designated as Sensitive Security Information, we can report we identified limitations with FAMS contributions to aviation security and a part of FAMS operations where, if discontinued, funds could be put to better use. [17]

We are in the midst of another round of covert testing across the country and

[15] *Covert Testing of TSA's Screening Checkpoint Effectiveness*, OIG-17-112 (September 2017).
[16] *TSA Penetration Testing of Advanced Imaging Technology (Unclassified Summary), OIG 12-06*; *Covert Testing of Access Controls to Secured Airport Areas, OIG-12-26*; *Vulnerabilities Exist in TSA's Checked Baggage Screening Operations (Unclassified Summary), OIG-14-142*; *Covert Testing of TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints (Unclassified Summary* (OIG-15-150).
[17] *FAMS' Contribution to Aviation Transportation Security is Questionable*, OIG-18-04 (September 2017).

have planned audits of the FAMS international flight operations and ground-based assignments. Consistent with our obligations under the *Inspector General Act*, we will report our results to this Committee as well as other committees of jurisdiction.

Right of First Refusal

A primary focus of the DHS OIG is the integrity of the 200,000 plus employees of the Department. Much of our investigative caseload concerns alleged corruption on the part of various DHS law enforcement personnel deployed along our borders with Mexico and Canada, TSA screeners, front line immigration services personnel, government contractors, etc.

While we applaud the DHS Authorization Act for implicitly granting the OIG the right of first refusal, our office suggests the language in the Act explicitly grants the OIG the right of first refusal to investigate allegations of criminal wrongdoing or other misconduct by DHS employees.

Inspectors General play a critical role in assuring transparent, honest, effective, and accountable government. Both the personal and organizational independence of OIG investigators, free to carry out their work without interference by agency officials, is essential to maintaining the public trust in not only the work of the OIG, but also in the DHS workforce as a whole. The American public must have a fundamental trust that government employees are held accountable for their crimes or serious misconduct by an independent fact finder.

DHS Management Directive (MD) 0810.1, The Office of Inspector General, implements the authorities of the Inspector General Act in DHS. MD 0810.1 establishes OIG's right of first refusal to conduct investigations of criminal misconduct by DHS employees and the right to supervise any such investigations conducted by DHS internal affairs offices. The MD requires that all allegations of criminal misconduct by DHS employees and certain other allegations received by the components—generally those against higher ranking DHS employees—be referred to OIG immediately upon receipt of the allegations. Many DHS components have an internal affairs office that conducts investigations. Under the authority of the IG Act, OIG has oversight responsibility for those internal affairs offices.

Mr. Chairman, this concludes my prepared statement. I welcome any questions you or other Members of the Committee may have.