STATEMENT OF RICHARD L. SKINNER

FORMER INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

U.S. SENATE

The Department of Homeland Security at 10 Years: A Progress Report on Management

March 21, 2013

Good afternoon Chairman Carper, Ranking Member Coburn, and Members of the Committee. It is truly an honor to be here today to discuss the progress that the Department of Homeland Security has made over the past 10 years and the challenges that remain in improving the management of the department. I thank you for this opportunity.

Since its inception in 2003, the department has worked strenuously to accomplish the largest reorganization of the federal government in more than half a century. Creating the third largest Cabinet agency with the missions of protecting the country against another terrorist attack, responding to threats and hazards, ensuring safe and secure borders, welcoming lawful immigrants and visitors, and promoting the free flow of commerce, has proven, to say the very least, a very difficult task. While the department has made commendable progress over the past 10 years developing and implementing initiatives to carry out its homeland security mission, it has moved at a much slower pace developing and implementing an integrated management platform to support those initiatives. Although progress is being made, it still has much to do to establish a cohesive, efficient, and effective organization.

Both the GAO's biennial update to its High-Risk Series report, dated February 14, 2013, and the DHS OIG's annual Major Management Challenges report, dated December 21, 2012, continue to highlight management support weaknesses that could adversely affect the department's ability to carry out its homeland security mission, ensure the effective and efficient use of limited resources, and provide accountability for its programs and operations. These challenges are essentially the same management challenges that both the GAO and OIG reported as early as 2005. Today, I would like to talk about four of them:

- Financial management
- Information technology management
- Acquisition management
- Grants management

These management support functions constitute the platform upon which the department's programs must operate and are critical to the accomplishment of the department's mission. The weaknesses associated with these support functions, for the most part, were inherited by the department from legacy agencies, and were compounded by the management and program challenges posed by the creation of a large, diverse, and complex organization. Also, the urgency and critical nature of the department's mission hampered efforts, at least in the early years, to focus on and build a strong, integrated management support foundation.

Senior officials at the department have recognized the significance of these challenges and understand that addressing them will take a sustained and focused effort. They have taken actions over the past several years to implement, transform, and strengthen the department's management support functions.

FINANCIAL MANAGEMENT

Financial management has been and continues to be a major management challenge for the department since its creation in 2003. The department has made progress from its early days, however. It has reduced the number of material weaknesses in internal controls from 18 to 5. It also received a qualified audit opinion on its consolidated balance sheet and custodial activity for the first time in fiscal year 2011. Unfortunately, unless it modernizes its financial systems, it is unlikely the department can sustain this progress. As the OIG pointed out in its 2012 Major Management Challenges report, achieving a qualified opinion resulted from the herculean efforts of the department's accountants, rather than reliance on a sound financial management system.

The department twice unsuccessfully attempted to implement an integrated department-wide financial management system, wasting millions of dollars. In 2007, the department ended its first attempt, the Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency system after determining it would not provide the expected functionality and performance. In 2011, the department decided to change its strategy for financial system modernization. Rather than implement a department-wide integrated financial management system solution, the department decided to take a decentralized approach to financial management systems modernization at the component level. Specifically, the department reported in its December 2011 strategy that it plans to replace financial management systems at three components it has identified as most in need, e.g., FEMA, USCG, and ICE. However, due to FY 2012 budget reductions, these initiatives have been put on hold indefinitely. It is now not clear when the department will resume its modernization strategy, nor is it clear whether this new, decentralized approach, if and whenever it is implemented, will ensure that components' financial management systems can generate reliable, useful, timely information for day-to-day decision making; enhance the department's ability to comprehensively view financial information across the department; and comply with related federal requirements at the department and its components. In the interim, the department must continue to use archaic, unreliable systems to manage it financial resources, which is unfortunate, particularly nowadays of budget austerity and the public demand for increased fiscal transparency and accountability.

INFORMATION TECHNOLOGY MANAGEMENT

Integrating the IT systems, networks, and capabilities of legacy agencies to form a single infrastructure for communications and information exchange remains one of the department's biggest challenges. It was by far, in my opinion, one of the department's biggest challenges when it was created in 2003. The department inherited thousands of IT systems from 22 legacy agencies. It took the department nearly 18 months just to inventory the number of systems that it had inherited. Many were are archaic and redundant, and almost all were not properly secured.

According to recent OIG and GAO reports, DHS and its components are still struggling to upgrade or transition their respective IT infrastructures, both locally and enterprise wide. For example, in November 2011, the OIG reported that US Citizen and Immigration Services delayed implementing its IT transformation program because of changes in the deployment strategy and system requirements that were insufficiently defined before selecting the IT system solution. Consequently, USCIS must rely on paper-based processes to support its mission, which makes it difficult to process immigration benefits efficiently, combat identity fraud, and share information promptly on possible criminals and terrorists.

Before his retirement in January 2012, the Assistant IG for Emergency Management Oversight, Matt Jadacki, testified before Congress that FEMA's existing information technology systems do not effectively support disaster response activities. FEMA had not completed its efforts to establish an enterprise architecture, and its IT strategic plan was not comprehensive enough to coordinate and prioritize its modernization initiatives and IT projects. The plan did not include clearly defined goals and objectives, nor did it address program office IT strategic goals. Without these critical elements, FEMA is challenged to establish an effective approach to modernize its information technology infrastructure and systems.

In June 2012, the OIG reported that the information technology environment and the aging IT infrastructure within CBP does not fully support CBP's mission needs. According to the OIG, interoperability and functionality of the technology infrastructure have not been sufficient to support CBP mission activities fully. As a result, CBP employees have created workarounds or employed alternative solutions, which may hinder CBP's ability to accomplish its mission and ensure officer safety.

More recently, in October 2012, the OIG completed an evaluation of the department's information security program and practices to comply with the requirements of the *Federal Information Security Management Act.* The OIG reported that DHS components still are not executing all the department's policies, procedures, and practices, and thereby weakening the department's overall information security posture.

Similar problems also have been reported at the Coast Guard, ICE, and Secret Service. Technical and cost barriers, aging infrastructure that is difficult to support, outdated IT strategic plans to guide investment decisions, and stove-piped system development have impeded the department's efforts to modernize and integrate its IT systems, networks, and capabilities.

Information Sharing

The Homeland Security Act of 2002 makes coordination of homeland security communication with state and local government authorities, the private sector, and the public a key department responsibility. However, due to time pressures, the department did not complete a number of the steps essential to effective planning and implementation of the Homeland Security Information Network (HSIN)—the "sensitive but unclassified" system it instituted to help carry out this mission. For example, the HSIN and the Homeland Security State and Local Community of

Interest systems, both developed by DHS, are not integrated. As a result, users must maintain separate accounts, and information cannot easily be shared across the systems. State and local fusion center personnel expressed concern that there were too many federal information sharing systems that were not integrated. As such, effective sharing of counter-terrorist and emergency management information critical remains an ongoing challenge for the department. Resources, legislative constraints, privacy, and cultural challenges—often beyond the control of the department—pose obstacles to the success of the department's information sharing initiatives.

On a broader scale, the department is also challenged with incorporating data mining into its overall strategy for sharing information to help detect and prevent terrorism. Data mining aids agents, investigators, and analysts in the discovery of patterns and relationships from vast quantities of data. The Homeland Security Act authorizes the department to use data mining and tools to access, receive, and analyze information. However, the department's data mining activities consist of various stove-piped activities that use limited data mining features. For example, CBP performs matching to target high-risk cargo. The Secret Service automates the evaluation of counterfeit documents. TSA collects tactical information on suspicious activities. ICE detects and links anomalies indicative of criminal activity to discover relationships. Without department-wide planning, coordination, and direction, the potential for integrating advanced data mining functionality and capabilities to address homeland security issues remains untapped.

I understand that DHS has taken numerous steps over the past 2 years to strengthen its enterprise architecture and information security programs. However, many of these initiatives are still a "work-in-progress." Much work remains to be done. The challenge for department from here-on-out will be sustaining the progress already made over the past few years while, at the same time, continuing to invest in improvements that are needed to strengthen its IT infrastructure.

ACQUISITION MANAGEMENT

During my tenure as the IG of the department, this was the one area that, in my opinion, improved the most. This was due, for most part, to the commitment made by the Secretary and Deputy Secretary of Homeland Security, and other senior officials, including my co-panelist, Elaine Duke, to improve the department's acquisition management function.

Beginning with the department's inception in 2003, the OIG and GAO identified perennial problems relating to acquisition oversight, cost growth, and schedule delays, resulting in performance problems and mission delays, as illustrated by the problems the department experienced with the Coast Guard's Deepwater program, CBP's SBINet program, FEMA's flood map modernization program, and the CFO's financial systems consolidation initiatives. Each of these efforts failed to meet capability, benefit, cost, and schedule expectations. For example, in June 2010 my former office reported that over half of the programs we reviewed awarded contracts to initiate acquisition activities without component or department approval of documents essential to planning acquisitions, such as mission need statements outlining the specific functional capabilities required to accomplish DHS's mission and objectives; operational

requirements; and acquisition program baselines. Additionally, the OIG reported that only a small number of DHS's major acquisitions had validated cost estimates.

Since the issuance of those reports, DHS has made remarkable strides to implement, transform, and strengthen its acquisition management capabilities. At the time of my retirement on March 1, 2011, the number of procurement staff had more than doubled since 2005. In addition, participation in the Acquisition Professional Career Program, which sought to develop acquisition leaders, increased 62% from 2008 to 2010. Also, since my retirement, according to GAO and the OIG, the department developed detailed plans to address a number of other acquisition management challenges. For example, it created a Procurement Staffing Model and chartered Centers of Excellence to enhance its acquisition capabilities, and is implementing a Decision Support Tool which was developed to gauge the health of major acquisitions and facilitate the flow of information from the components to the Management Directorate. Furthermore, I think it is worth mentioning, DHS reduced its noncompetitive contracts over the past four years by 89 percent, from $3.5 billion in 2008 to $389 million in fiscal year 2012. In my opinion, this is a major accomplishment.

However, as both the GAO and OIG have pointed out over the past year, much work remains. The department continues to experience performance problems, cost overruns, schedule delays, and often lacks fundamental documents needed to help manage risk and measure performance. Both the GAO and OIG have recommended that the department equip the Office of the Chief Procurement Officer with additional resources to provide effective, department-wide oversight of acquisition policies and procedures, and the authority to enforce compliance with those policies and procedures. To be truly successful, the department must have an infrastructure in place that not only enables it to effectively oversee the complex and large dollar procurements critically important to achieving its mission, but also provides the transparency, accountability, and enforcement tools needed to ensure that its components are adhering to key knowledge-based acquisition practices and departmental policies and procedures.

The urgency and complexity of the department's mission will continue to demand rapid pursuit of major investment programs. Since its creation, the department spent about 40% of its budget on contracts. In fiscal year 2012, the department had approximately 160 acquisition programs with estimated life cycle costs of more than $144 billion. Although that figure may decrease in the years ahead, the department will continue to rely heavily on contractors to accomplish its multifaceted mission and will continue to pursue high-risk, complex acquisition programs.

GRANTS MANAGEMENT

Disaster Grants Management

FEMA oversees billions of dollars in disaster grant funds each year, and, due to the environment under which these funds are administered, they are highly vulnerable to fraud, waste, and abuse. To illustrate, during fiscal year 2012, the OIG's audits of 56 disaster grants identified $387 million in questionable costs and funds that could be put to better use. The extent of the fraud,

waste, and abuse that the OIG uncovers year after year in the disaster relief program, for the past 25 years, is unacceptable, and it needs to be vigorously addressed. Yet FEMA still has not developed a robust program to curtail fraud, waste, and abuse within its disaster relief programs.

Preparedness Grants Management

Over the past 10 years, DHS has awarded more than $35 billion to state, local, tribal, and territorial governments to enhance their capabilities to prepare for and prevent natural and manmade disasters and acts of terrorism.

Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007, requires the OIG to audit individual states' management of State Homeland Security Program and Urban Areas Security Initiatives grants and annually submit to Congress a report summarizing the results of these audits. In the audits completed to date, the OIG concluded that the states have generally done an efficient and effective job of administering the grant management program requirements, distributing grant funds, and ensuring that all the available funds were used.

However, according to an OIG report released this past December, the department still does not have a system in place to determine the extent its preparedness grants have enhanced the states' capabilities to prevent, deter, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Also, the department does not require states to report progress in achieving milestones as part of the annual application process. As a result, when annual application investment justifications for individual continuing projects are being reviewed, DHS does not know whether prior year milestones for the projects have been completed. DHS also does not know the amount of funding required to achieve needed preparedness and response capabilities. Furthermore, many states have outdated strategic plans, and many do not have plans with goals and objectives that are specific, measurable, achievable, results-oriented, and time-limited. Without some form of measurable goal or objective, or a mechanism to objectively gather results-oriented data, neither DHS nor the states can demonstrate the level of effectiveness of the Nation's preparedness and response capabilities.

Finally, DHS needs to improve its grantee monitoring program to ensure the grant recipients are meeting their financial and project obligations on time and according to applicable federal and state laws and regulations. On February 14, 2013, the OIG reported that DHS either inconsistently applied or failed to apply risk indicators to determine the level of monitoring a grantee should receive. Consequently, DHS did not have a reasonable level of assurance that high-risk grantees were being monitored.

Strategic planning, performance measurement, and oversight are important management controls for DHS to ensure that federal funds are used for their intended purpose and that enhancements in preparedness capabilities are being achieved. Without a bona fide performance measurement system, it is impossible to determine whether annual investments are improving our Nation's homeland security posture. Furthermore, without clear, meaningful performance standards, the

department lacks the tools necessary to make informed funding decisions. In today's economic climate, it is critical that DHS concentrate its limited resources on those threats that pose the greatest risk to the country.

****

In conclusion, I believe it is important to understand that most, if not all, of the department's management support challenges were inherited from the department's legacy agencies. The department did not create them. To compound matters, the complexity and urgency of the department's mission have often exacerbated the department's ability to address them in a disciplined and effective manner.

The department's senior officials are well aware of these challenges and are attempting to remedy them, and, are making some headway. Today, ten years after its creation, the department now has in place one of the strongest management teams imaginable. The Under Secretary for Management, the Chief Information Officer, the Chief Financial Officer and the Chief Procurement Officer, all have proven that they possess the knowledge and skills needed to get the job done. Moreover, they have the full support of the Secretary and Deputy Secretary, both of whom have demonstrated a their commitment to improving the department's management functions.

The question now is does the department have the resolve and wherewithal to sustain those efforts. The ability of the department to do so is fragile, not only because of the early stage of development that the initiatives are in, but also because of the government's budget constraints and the current lack of resources to implement planned corrective actions. In today's environment of large government deficits and pending budget cuts, the new challenge will be to sustain the progress already made and at the same time continue to make the necessary improvements that are critical to the success of the department's management functions and, what is more important, to its homeland security mission. To accomplish this, they need your support.

It is important that the Congress continue to invest in the department's management improvement initiatives, and continue to provide oversight of those efforts. Unless the department and Congress stay focused on these challenges, it will be harder than ever to facilitate solutions to strengthen the department's management support functions and, ultimately, its homeland security mission.

Mr. Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or the Members may have.

****