STATEMENT OF ANNE L. RICHARDS

ASSISTANT INSPECTOR GENERAL FOR AUDITS

DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

COMMITTEE ON HOMELAND SECURITY

U.S. HOUSE OF REPRESENTATIVES

CONCERNING

"CUTTING DHS DUPLICATION AND WASTEFUL SPENDING: IMPLEMENTING PRIVATE SECTOR BEST PRACTICES AND WATCHDOG RECOMMENDATIONS"

APRIL 26, 2013

Chairman Duncan, Ranking Member Barber, and Members of the Subcommittee, thank you for inviting me here today to discuss cutting duplication and wasteful spending, and implementing private sector best practices and watchdog recommendations at the Department of Homeland Security (DHS).

My testimony today will address some of our high priority short and long-term open recommendations we have made to DHS, which were included in reports issued between December 2011 and December 2012.

In the 10 years since its establishment, DHS has matured and made progress in addressing challenges to accomplishing its mission, and it has laid the groundwork to manage its resources effectively. However, to fulfill its vital mission of protecting and securing our Nation successfully, the Department must continue to overcome challenges that hinder its efforts. The high-priority open recommendations from the reports discussed below illustrate our efforts to assist DHS and its components in addressing and overcoming the most persistent challenges they face. We believe that by implementing these recommendations, DHS will continue to improve the effectiveness and efficiency of its operations and reduce the potential for waste and duplication of effort.

Background

Since DHS-OIG's inception we have made over 8000 recommendations to the Department and its components identifying over $2.6 billion in questioned costs, unsupported costs, or funds that could be put to better use. Approximately 15% of these recommendations remain open, representing about $650 million.

Our December 2012 report, *Major Management Challenges Facing the Department of Homeland Security – Revised*, summarized and assessed the Department's progress in addressing its most serious management challenges. We grouped these challenges into the mission areas of intelligence, transportation security, border security, infrastructure protection, and disaster preparedness and response; and accountability issues of acquisition management, financial management, IT management, grants management, employee accountability and integrity, and cybersecurity.

Border Security

Our report, *CBP's Use of Unmanned Aircraft Systems in the Nation's Border Security* (OIG-12-85), issued in May 2012, covered our audit of U.S. Customs and Border Protection's (CBP) efforts to establish a program for its unmanned aircraft systems (UAS). In this report, we made a recommendation to improve CBP's UAS program planning, which is still open and considered a high-priority short-term recommendation. In November 2012, we issued a report, *DHS' Oversight of Interoperable Communications* (OIG 13-06), which includes a high-priority, short-term open recommendation that DHS establish policies and procedures to standardize radio communications.

CBP's Program for Unmanned Aircraft Systems

CBP's Office of Air and Marine (OAM) is responsible for protecting the American people and the Nation's critical infrastructure through the coordinated use of integrated air and marine forces. Air and marine forces are used to detect, interdict, and prevent acts of terrorism and the unlawful movement of people, illegal drugs, and other contraband toward or across U.S. borders. UASs provide command, control, communication, intelligence, surveillance, and reconnaissance capability to complement crewed aircraft and watercraft, and ground interdiction agents.

After the pilot of the UAS program, Congress appropriated more than $240 million to establish the program within CBP. During our 2012 audit, CBP stated it had expended $152.3 million to purchase nine unmanned aircraft and related equipment and, at that time, had seven operational aircraft. After our audit, in late 2011, CBP received two additional aircraft and was awaiting delivery of a tenth aircraft purchased with fiscal year (FY) 2011 funds. Each aircraft system cost approximately $18 million.

We reported that CBP had not adequately planned resources needed to support its current unmanned aircraft inventory. Although CBP developed plans to use the unmanned aircraft's capabilities to fulfill OAM's mission, its Concept of Operations planning document did not sufficiently address processes (1) to ensure that required operational equipment, such as ground control stations and ground support equipment, was provided for each launch and recovery site; (2) for stakeholders to submit unmanned aircraft mission requests; (3) to determine how mission requests would be prioritized; and (4) to obtain reimbursements for missions flown on stakeholders' behalf. With this approach, CBP risked having invested substantial resources in a program that underutilized assets and limited its ability to achieve OAM mission goals.

Because UAS is critical to protecting the American people and our infrastructure, CBP needed to improve its planning to address the UAS program's level of operation, funding, and resource requirements, along with stakeholder needs. Thus, we recommended that CBP analyze requirements and develop plans to achieve the UAS mission availability objective and acquire funding to provide necessary operations, maintenance, and equipment.

DHS' Oversight of Interoperable Communications

DHS includes a network of organizations that work together to prevent and respond to terrorist attacks, other threats, and natural disasters. Such collaboration requires that DHS components establish effective communication among external and internal partners during operations. DHS established an internal goal of developing interoperable radio communications and identified common channels. To meet communications requirements, DHS components invested about $430 million in equipment, infrastructure, and maintenance. Although DHS created policies, guidance, and templates to aid in achieving interoperability and provided more than $18 million in assistance to State and local agencies, full interoperability remains a distant goal, according to a 2012 Government Accountability Office report.[1]

[1] *Emergency Communications-Various Challenges Likely to Slow Implementation of a Public Safety Broadband Network* (GAO-12-343, February 2012).

In our November 2012 report we noted that, although DHS had established a goal for interoperability and common radio channels, only 1 of 479 radio users we reviewed could access and communicate using the specified channel. Furthermore, only 78 of 382 or 20 percent of radios that we tested contained all the correct program settings, including the name, for the common DHS channel. Additionally, DHS did not establish an effective governing structure with authority and responsibility to oversee achievement of department-wide interoperability. Without an authoritative governing structure to oversee emergency communications, DHS had limited interoperability policies and procedures, and the components did not inform radio users of DHS-developed guidance.

Because of this limited progress in interoperability, personnel could not rely on interoperable communications during daily operations, planned events, and emergencies. We recommended that DHS create a structure with the necessary authority to ensure that the components achieve interoperability and to develop and disseminate policies and procedures to standardize department-wide radio activities, including program settings, such as naming conventions, to ensure interoperability.

Disaster Preparedness and Response

Our December 2011 report, *FEMA's Process for Tracking Public Assistance Insurance Requirements* (OIG-12-18), includes a high-priority, long-term recommendation to help resolve longstanding insurance-related issues. In January 2012, we issued a report related to Federal Emergency Management Agency's (FEMA) response to Hurricane Katrina, *Efforts to Expedite Disaster Recovery in Louisiana* (OIG-12-30), in which we made a short-term and a long-term recommendation, both related to closing out Public Assistance (PA) projects and both of which we consider high-priority and both are open.

<u>FEMA's Process for Tracking Public Assistance Insurance Requirements</u>

FEMA's PA grants totaled more than $10 billion for all disasters declared between 2007 and 2010. Of that amount, the component provided $1.3 billion for buildings, contents, and equipment owned by State, tribal, and local governments, as well as by private nonprofit organizations. Since FY 2009, we have issued 19 financial assistance grant reports that included findings pertaining to PA insurance requirements, which involved duplicate benefits, incomplete insurance reviews, and applicants who either did not obtain adequate insurance or did not file an insurance claim.

The *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (Stafford Act) encourages State and local governments to protect themselves by obtaining insurance to supplement or replace Federal Government assistance. To receive PA grant funding and be eligible for funding in future disasters, the Stafford Act also requires applicants to obtain and maintain insurance on damaged insurable facilities. However, FEMA's PA program includes disincentives for applicants to carry insurance. For example, the program pays for building repair following a first disaster, which reduces the incentive for building owners to purchase insurance if they have not previously received disaster assistance. In addition, FEMA reimburses deductible amounts in

insurance policies, regardless of the amount of the deductible, which encourages high deductibles.

FEMA has been aware of these and other equity issues and disincentives for more than a decade. In February 2000, FEMA published an advance notice of proposed rulemaking in the *Federal Register* that addressed insurance requirements, procedures, and eligibility criteria with respect to buildings under the PA program. However, FEMA has not issued a final rule and stated that these issues have not been acted on because regulatory review and rulemaking for other programs have taken precedence. Consequently, the disincentives and equity issues continue, and PA program regulations do not provide adequate guidance to those who receive, grant, or oversee PA grants.

In our December 2011 report, we recommended that FEMA complete the rulemaking process begun in 2000 and issue a final rule that resolves the longstanding issues with PA insurance regulations, including those related to deductibles, self-insurance, and state insurance commissioners' determinations of reasonably available insurance. In February 2013, FEMA rescinded the policy of reducing eligible costs by an insurance deductible by deducting all insurance proceeds received or anticipated from the total eligible cost of the project. This change in policy provides further incentive for applicants to not carry insurance or, if they do, to choose the highest deductible possible.

FEMA's Efforts to Expedite Disaster Recovery in Louisiana

Under the authority of the Stafford Act, FEMA provides Federal disaster grant assistance to State, tribal, and local governments and certain private nonprofit organizations through the PA program. FEMA has an obligation to ensure timely and appropriate use of Federal disaster funds. In January 2012, we reported that only 6.3 percent of the PA projects for Louisiana had been closed out in the 6 years since Hurricane Katrina made landfall. Many of these projects are years past the closeout deadlines.

Although FEMA has worked with Louisiana to expedite the recovery effort, several factors have contributed to the slowness in closing out PA projects. Specifically, the Federal Government provided 100 percent funding of PA projects. The State of Louisiana does not pay for projects and has no incentive to seek cost-effective replacement or repair solutions, close completed projects, or reduce the disaster workforce as work is completed. Other factors, such as the project procurement process, inconsistent decisions for applicant eligibility, and determining whether to replace or repair, as well as limited State staff resources, also contributed to delays in closing PA projects.

Because open PA projects could involve substantial amounts of obligated Federal funds that could be put to better use, we recommended in the short-term, that FEMA develop and implement specific policies, procedures, and timelines to ensure timely closeout of 100 percent federally funded projects. For the long-term, we recommended that FEMA evaluate the status of all PA projects in Louisiana associated with Hurricane Katrina and develop, in conjunction with the State, a process to close completed projects and to expedite the completion of open projects.

FEMA took several actions to respond to our recommendations. Specifically, the component completed the draft of an updated standard operating procedure for PA program management and grant closeout. In addition, FEMA began implementing a training course, which was scheduled for a pilot release in FY 2013, to address the PA program process and the roles and responsibilities for closeout activities. FEMA also developed a procedure to track the progress of recovery and the movement toward programmatic closeout of Hurricanes Katrina, Rita, Gustav, and Ike projects.

FEMA also worked with the State of Louisiana, which developed a closeout process to ensure that each applicant and project met the eligibility requirements and document standards mandated by Federal and State regulations. In addition, FEMA developed and communicated clear goals for subgrantees to certify that projects were completed, which provide an incentive for meeting these goals. FEMA conducted a complete review of the project closeout process used by the state. The average number of projects closed monthly increased by 300 percent for Hurricanes Katrina and Rita in the first quarter of FY 2013. We will review these efforts to determine whether they have successfully resolved the recommendations.

Financial Management

DHS is responsible for an annual budget of more than $59 billion, employs more than 225,000 men and women and operates in more than 75 countries. Sound financial practices and related management operations are critical to achieving the Department's mission and to providing reliable, timely financial information to support management decision-making throughout DHS. Although DHS produced auditable financial statements in FY 2012 and obtained a qualified opinion on those statements, challenges remain for the Department's financial management. One high-priority, long-term challenge is the improvement of the Department's financial management systems.

Independent Auditors' Report on DHS' FY 2012 Financial Statements and Internal Control over Financial Reporting

An independent public accounting firm, KPMG LLP, performed the integrated audit of the DHS financial statements for FY 2012 and an examination of internal control over financial reporting and compliance.[2] KPMG considered the effects of financial system functionality in its tests and determined that many key DHS financial systems are not compliant with the *Federal Financial Management Improvement Act of 1996* (FFMIA) and Office of Management and Budget Circular Number A-127, *Financial Management Systems*, as revised. DHS financial system functionality limitations add substantially to the Department's challenges of addressing systemic internal control weaknesses, as well as limit its ability to leverage IT systems to process and report financial data effectively and efficiently.

[2] DHS-OIG, *Independent Auditors' Reports on DHS' FY08, 09, 10, 11, and 12 Financial Statements and Internal Control Over Financial Reporting* (OIG-09-09, November 2008; OIG-10-11, November 2009; OIG-11-09, November 2010; OIG-12-07, November 2011; OIG-13-20, November 2012).

Specifically, KPMG identified the following persistent, pervasive financial system functionality issues:

- An inability to process, store, and report financial and performance data to facilitate decision-making, safeguarding and management of assets, and preparation of financial statements that comply with generally accepted accounting principles.

- Technical configuration limitations, such as outdated systems that software vendors can no longer fully support, that impair DHS' ability to comply with policy in areas such as IT security controls, audit logging, user profile changes, and restricting departing employees' and contractors' access.

- System capability limitations that prevent or restrict the use of applications controls to replace less reliable, more costly manual controls. In some cases, additional manual controls must compensate for IT security or control weaknesses.

Additionally, KPMG determined that the United States Coast Guard (USCG):

- Is routinely unable to query its various general ledgers to obtain a population of financial transactions and consequently, must create many manual custom queries that delay financial processing and reporting processes.

- Has a key financial system that is limited in processing overhead cost data and depreciation expenses to support the property, plant, and equipment financial statement line item.

- Uses production versions of financial statements that are outdated and do not provide the necessary core functional capabilities (e.g., general ledger capabilities).

- Has a budgetary module of the core financial system that is not activated. As a result, key attributes (e.g., budget fiscal year) are missing and potential automated budgetary entries (e.g., upward adjustments) are not used. This has created the need for various manual workarounds and nonstandard adjustments.

- Has a financial systems functionality limitation that is preventing the component from establishing automated processes and application controls to improve accuracy and reliability, and to facilitate efficient processing of certain financial data, such as receipt of goods and services upon delivery and ensuring proper segregation of duties and access rights.

KPMG concluded in its report that these findings limit DHS' ability to process, store, and report financial data in a manner that ensures accuracy, confidentiality, integrity, and availability. KPMG emphasized that some of these weaknesses may result in material errors in financial data that go undetected through the normal course of business. Additionally, because of financial system functionality weaknesses, there is added pressure on mitigating controls to operate effectively. Mitigating controls are often more manual, which increases the risk of human error that could materially affect the financial statements. We recommended that the DHS Office of the Chief Information Officer, in conjunction with the Office of the Chief Financial Officer,

continue the Financial Systems Modernization initiative and make necessary improvements to the Department's financial management systems.

IT Management

As technology constantly evolves, the protection of the Department's IT infrastructure becomes increasingly important. The Department's Chief Information Officer has taken steps to mature IT management functions, improve IT governance, and integrate IT infrastructure.

Cybersecurity

The firewall of cybersecurity—the technologies, processes, and practices that protect our systems from attack, damage, or unauthorized access—is always on alert for threats to networks, computers, programs, and data. In 2012, we recommended actions to address weaknesses in DHS' international cybersecurity program.

DHS' International Cybersecurity Program

Our Nation's economy and security are highly dependent on the global cyber infrastructure. The borderless nature of threats to, and emanating from, cyberspace requires robust engagement and strong partnerships with countries around the world. International engagement is a key element of the DHS cyber mission to safeguard and secure cyberspace. DHS' National Protection and Programs Directorate (NPPD) promotes cybersecurity awareness and fosters collaboration with other countries and organizations to global cyber space threats.

In our report *DHS Can Strengthen Its International Cybersecurity Programs* (OIG-12-112), which we issued in August 2012, we reported that NPPD had undertaken actions to promote collaboration with the international community and develop partnerships with other nations to protect cyberspace better. However, NPPD had not defined its roles for carrying out the mission of its international affairs program, nor had it developed a strategic implementation plan to provide a clear plan of action for achieving its cybersecurity goals with international partners, international industry, or the private sector. In addition, NPPD had not streamlined its international affairs functions and processes to support its international cybersecurity goals, objectives, and priorities efficiently, nor had had it effectively consolidated resources. Lastly, NPPD needed to strengthen its communications and information sharing activities with international partners to promote international incident response, exchange of cyber data with other nations, and to share best practices. We recommended that DHS develop and implement policies and procedures for establishing and maintaining open dialogues with foreign partners regarding cyber threats and vulnerabilities.

Steps Taken to Implement High-Priority Recommendations

DHS and its components are taking steps to implement these high-priority recommendations to improve and strengthen program management with which it agreed. In most instances, however, particularly for long-term recommendations, it takes time to develop plans, revise and update guidance, and implement and disseminate new policies and procedures. This can be particularly time-consuming when, as is usually the case, such plans, policies, and procedures require

coordination and concurrence among multiple entities, including some outside of DHS and its components. Competing and changing priorities and funding uncertainties also affect the Department's ability to implement multiple recommendations quickly. In addition, some recommended improvements require funding and staffing resources that are not readily available.

Although DHS has made a number of attempts over the years to improve and integrate its financial systems, for various reasons, it has not yet successfully completed this complicated task. For example, because of a vendor protest, a contract for an enterprise-wide initiative had to be cancelled. In addition, in June 2010, the Office of Management and Budget (OMB) required all agencies to halt the issuance of new task orders or new procurements for all financial system projects pending its review and approval. In an effort to comply with the OMB requirement, DHS began upgrading existing financial systems at some components. Projects aimed at improving financial and IT systems are scheduled to be implemented at the USCG and FEMA in FY 2013.

Questioned Costs

From April 1, 2012 through September 30, 2012, our audits resulted in questioned costs of more than $235 million. During this same period, DHS recovered approximately $115 million as a result of disallowed costs identified in current and previous audit reports and from our investigative efforts. We issued 12 reports identifying approximately $101 million in funds that could be put to better use.

Conclusion

We encourage Congress and this subcommittee to continue its oversight of DHS and its components to ensure effective and efficient program management and sound financial practices. For our part, we will continue to analyze the Department's programs and practices to identify those that need improvement, determine how DHS and its components can address deficiencies and weaknesses, and recommend appropriate solutions to strengthen the Department. We understand that our recommended corrective actions will strengthen DHS only if they are implemented. Therefore, we will also continue our efforts to follow up with the Department to make certain that it carries out its mission as effectively and efficiently as possible.