STATEMENT OF CHARLES K. EDWARDS

DEPUTY INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

MARCH 19, 2013

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to discuss ways to reduce waste and improve efficiency at the Department of Homeland Security (DHS).

My testimony today will address DHS' high priority open recommendations for both the short term and long term. The open recommendations we identified as the highest priority were in eight reports issued between December 2011 and December 2012. These recommendations address critical mission areas, such as the security of our Nation's borders, information sharing to accomplish intelligence and other Department goals, and the response to and recovery from natural disasters. The recommendations also address critical accountability issues, such as financial management, information technology (IT) management, and cybersecurity.

As DHS continues to mature as a Department, it has made progress in addressing its key mission areas and establishing the groundwork for effective stewardship over its resources; yet challenges remain. The open recommendations discussed today illustrate some of the ongoing challenges facing DHS and its component offices. Once these recommendations are addressed, DHS will be in a better position to improve the effectiveness and efficiency of its operations and reduce the potential for waste, fraud, and mismanagement.

Background

As of March 8, 2013, DHS OIG has issued 8,068 of recommendations since its inception in March 2003, and 1,253 (16 percent) of those recommendations remain open. Of the open recommendations, 210 have monetary findings associated with them of $1.2 billion.

In December 2012, we issued our Major Management Challenges report, which summarized and briefly assessed progress of the most serious challenges facing the Department.[1] These challenges were categorized into two main themes: Mission Areas—Intelligence, Transportation Security, Border Security, Infrastructure Protection, and Disaster Preparedness and Response; and Accountability Issues—Acquisition Management, Financial Management, IT Management, Grants Management, Employee Accountability and Integrity, and Cyber Security.

On December 5, 2012, we received a request from this Committee to identify our office's five highest priority short-term and five highest priority long-term open recommendations to improve agency efficiency and reduce waste; and to describe whether and in what ways DHS management solicits input on how to improve efficiency and reduce waste. We provided this information in a written response on February 11, 2013, identifying our short- and long-term high-priority recommendations; eight of which were also included in our 2012 Major Management Challenges.

[1] DHS OIG, *Major Management Challenges Facing the Department of Homeland Security-Revised* (OIG-13-09, December 2012).

Five of the 10 high-priority open recommendations focus on DHS mission areas of border security, intelligence, and disaster preparedness and response. The remaining five high-priority open recommendations focus on accountability issues of financial management, IT management, and cybersecurity.

Mission Area: Border Security

Securing the Nation's borders from illegal entry of aliens and contraband, including terrorists and weapons of mass destruction continues to be a major challenge. Within DHS, the United States Customs and Border Protection (CBP) is responsible for securing the Nation's borders at and between the ports of entry.

In an effort to accomplish this mission, DHS needs to improve its unmanned aircraft system program. In 2012, we made a high-priority short-term recommendation to improve CBP's program for its unmanned aircraft system (UAS). Also in 2012, we made one high-priority short-term recommendation to address interoperable communications oversight.

CBP's Use of Unmanned Aircraft Systems in the Nation's Border Security

The mission of CBP's Office of Air and Marine (OAM) is to protect 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. The UAS provides 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 a UAS program within CBP. During our 2012 review, CBP stated it had expended $152.3 million to purchase nine aircraft and related equipment, and it had seven operational aircraft. CBP received 2 additional aircraft in late 2011 and was awaiting delivery of a tenth aircraft purchased with 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 in its OAM mission, its Concept of Operations planning document did not adequately address processes (1) to ensure that required operational equipment, such as ground control stations and ground support equipment, is provided for each launch and recovery site; (2) for stakeholders to submit unmanned aircraft mission requests; (3) to determine how mission requests are prioritized; and (4) to obtain reimbursements for missions flown on stakeholders' behalf. This approach places CBP at risk of having invested substantial resources in a program that underutilizes resources and limits its ability to achieve OAM mission goals.

Because UAS is a critical aspect of protecting the American people and the Nation's infrastructure, CBP needs to improve the planning of its UAS program to address its level

of operation, program funding, and resource requirements, along with stakeholder needs. 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.[2]

DHS' Oversight of Interoperable Communications

The establishment of DHS in 2003 created a network Federal departments and agencies that work together to prevent and respond to terrorist attacks, natural disasters, and other threats. The Department set a goal that all components would be able to communicate using interoperable radio systems, and it planned to achieve that goal by establishing a common radio channel and purchasing standardized equipment. Even though 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.[3]

In fact, in November 2012, we also reported 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 (20 percent) radios 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 the achievement of Department-wide interoperability. Without an authoritative governing structure to oversee emergency communications, DHS has limited interoperability policies and procedures.

Because of this limited progress in interoperability, personnel do not have interoperable communications to rely on during daily operations, planned events, and emergencies. We recommended that DHS develop and disseminate policies and procedures to standardize Department-wide radio activities, including program settings, such as naming conventions, to ensure interoperability.[4]

Mission Area: Disaster Preparedness and Response

The Federal Emergency Management Agency's (FEMA) task of coordinating emergency support following disasters has become more challenging as the number of events to which it responds has risen each year-from 25 to 70 since 1980. From 2008 through 2011, FEMA obligated an average of $9.5 billion each year in its response efforts. Although the agency has improved its disaster response and recovery, challenges remain. In late 2011 and early 2012, we issued two reports relating to FEMA's response to Hurricane Katrina. One report contained two high priority recommendations – one short-term and one long-term– relating to FEMA's efforts to expedite disaster recovery in

[2] DHS-OIG, *CBP's Use of Unmanned Aircraft Systems in the Nation's Border Security* (OIG-12-85, May 2012).
[3] *Emergency Communications-Various Challenges Likely to Slow Implementation of a Public Safety Broadband Network* (GAO-12-343, February 2012).
[4] DHS-OIG, *DHS' Oversight of Interoperable Communications* (OIG-13-06, November 2012).

Louisiana. The second report contained a high-priority recommendation to improve FEMA's process for tracking public assistance insurance in the long term.

Efforts to Expedite Disaster Recovery in Louisiana

Under the authority of the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, as amended (*Stafford Act*), FEMA provides Federal disaster grant assistance to state, tribal, and local governments and certain private nonprofit organizations through the Public Assistance (PA) program. FEMA has an obligation to ensure that Federal disaster funds are used appropriately and timely. 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 slow progress of closing out PA projects. Specifically, the Federal Government provided 100 percent funding of PA projects. The State of Louisiana does not pay the project costs and has no incentive to seek cost effective replacement or repair solutions, close completed projects, or begin reducing the disaster workforce as work is completed. Other factors, such as the project procurement process, inconsistent decisions for applicant eligibility and replacement versus repair determines early in the PA process, and limited state staff resources also contributed to delays in closing PA projects.

Because open PA projects could involve substantial amounts of obligated Federal dollars that could be put to better use, we recommended that FEMA develop and implement specific policies, procedures, and timelines to ensure that 100 percent federally funded projects are closed timely in the short term. Regarding long-term high priority challenges, we recommended that FEMA evaluate the status of all PA projects in Louisiana associated with Hurricane Katrina; and develop, in conjunction with Louisiana, a process to close completed projects and to expedite the completion of open projects.[5]

FEMA has taken several actions to respond to our recommendations. Specifically, FEMA has completed the draft of an updated standard operating procedure for PA program management and grant closeout. In addition, FEMA is implementing a training course, scheduled for a pilot release in FY 2013, to address the PA program process and the roles and responsibilities for closeout activities. FEMA has 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 has worked with the State of Louisiana, which developed a closeout process to ensure that each applicant and project meet the eligibility requirements and document standards mandated by Federal and State regulations. In addition, FEMA developed and communicated clear goals for subgrantee certification of project completion, which provide a closeout incentive if certification goals are met. FEMA conducted a complete review of the project closeout process used by the state. The average number of projects

[5] DHS-OIG, *Efforts to Expedite Disaster Recovery in Louisiana* (OIG-12-30), January 2012.

closed monthly has increased by 300 percent for Hurricanes Katrina and Rita in the first quarter of FY 2013. We will be reviewing these efforts to see whether they have successfully resolved the recommendations.

FEMA's Process for Tracking Public Assistance Insurance Requirements

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

The *Stafford Act* encourages states and local governments to protect themselves by obtaining insurance to supplement or replace government assistance, and requires applicants to obtain insurance on damaged insurable facilities as a condition of receiving PA grant funding, and to maintain insurance on those facilities in order to be eligible for PA funding in future disasters. Yet FEMA's PA program provides disincentives for applicants to carry insurance. For example, the PA program pays for building repair costs 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 and disincentive problems 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 action on these issues has not occurred because regulatory review and rulemaking involving other programs have taken precedence. Consequently, the pertinent PA regulations continue to present the same disincentives and equity issues, and do not provide adequate guidance to those involved in receiving, granting, or overseeing PA grants.

In December 2011, we recommended that FEMA complete the rulemaking process begun in 2000 and issue a final rule that resolves the longstanding problems with PA insurance regulations, including the topics of deductibles, self-insurance, and state insurance commissioners' determinations of reasonably available insurance, among others.[6] However, in February 2013, FEMA issued a memorandum rescinding the policy of reducing eligible costs by an insurance deductible. Effective immediately, FEMA deducts total 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.

[6] DHS-OIG, *FEMA's Process for Tracking Public Assistance Insurance Requirements* (OIG-12-18, December 2011).

Accountability Issue: Financial Management

DHS is responsible for an annual budget or 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 fiscal year 2012 and an examination of internal control over financial reporting and compliance. KPMG considered the effects of financial system functionality in its tests, and determined that many key DHS financial systems are not compliant with Federal Financial Management Improvement Act of 1996 (FFMIA) and OMB 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, and limit the Departments ability to leverage IT systems to effectively and efficiently process and report financial data.

Specifically, KPMG identified persistent and pervasive financial system functionality conditions at all of the significant DHS components in the following areas:

- Inability of financial systems to process, store, and report financial and performance data to facilitate decision making, safeguarding and management of assets, and prepare financial statements that comply with generally accepted accounting principles.
- Technical configuration limitations, such as outdated systems that are no longer fully supported by the software vendors, impaired DHS' ability to fully comply with policy in areas such as IT security controls, notably password management, audit logging, user profile changes, and the restricting of access for off-boarding employees and contractors.
- System capability limitations prevent or restrict the use of applications controls to replace less reliable, more costly manual controls. Or in some cases, require additional manual controls to compensate for IT security or control weaknesses.

Additionally, KPMG determined that the U.S. Coast Guard:

- 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 in support of 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 the implementation of nonstandard adjustments.
- Has financial systems functionality limitations that are preventing the Coast Guard from establishing automated processes and application controls that would improve accuracy, reliability, and facilitate efficient processing of certain financial data; like 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 in its ability to process, store, and report financial data in a manner to ensure 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. Because mitigating controls are often more manually focused, there is an increased 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.[7]

Accountability Issue: IT Management

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

[7] 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).

challenges. In 2012, we issued a high priority long-term recommendation to address a Customs and Border Protection (CBP) IT management challenge.

CBP Information Technology Management Challenges

IT systems play a critical role in enabling CBP to accomplish its border security, trade, and travel missions. To support its mission, CBP had an IT budget of $1.5 billion in fiscal year 2012, making it the component with the largest IT budget within the Department.

In June 2012, we reported that the CBP Chief Information Officer has taken several actions to support effective IT management by implementing a strategic planning process, developing an enterprise architecture, and establishing a systems engineering life cycle process to guide and manage CBP's information technology environment. However, system availability challenges exist, due in part to aging infrastructure. Also, 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. We recommended that CBP implement a plan to address gaps in the existing requirements and reassess the technology insertion process to address functionality and interoperability challenges in the field.[8]

Accountability Issue: Cybersecurity

Cybersecurity is our Nation's firewall because it is always on alert for constant threats to networks, computers, programs, and data. It contains technologies, processes, and practices that protect our systems from attack, damage, or unauthorized access. In 2012, we made three high priority recommendations – two to address the Transportation Security Administration's (TSA) insider threat challenges in the short-term, and one high priority long-term recommendation to address weaknesses in DHS' International Cybersecurity Programs.

TSA Insider Threat Challenges

TSA relies on sensitive transportation security information to meet its mission of protecting the Nation's transportation systems. TSA employees, contractors, and partners have access to TSA's operations, systems, and data. Based on job function, these trusted insiders are typically given unfettered or elevated access to mission-critical assets. This access creates potential vulnerability to insider threats, such as spying, release of information, sabotage, corruption, impersonation, theft, smuggling, and terrorist attacks.

We reported in July 2012 that TSA has taken steps to reduce the risk of insider threats by establishing an agency-wide Insider Threat Working Group and Insider Threat Section responsible for implementing a program to address insider threat risk. However, TSA had not yet implemented protective measures to detect or prevent unauthorized removal or copying of sensitive information via portable media devices or unauthorized exfiltration of sensitive information outside TSA's network. We recommended that TSA

[8] DHS-OIG, *CBP Information Technology Management: Strengths and Challenges* (OIG-12-95, June 2012).

disable USB ports, which can be used to transfer data, on desktop and laptop computer if there is not a legitimate business need for them to be activated. We also recommended that TSA limit the size of e-mail file attachments if there is not a legitimate business need for such attachments.[9]

DHS' International Cybersecurity Programs

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 cyberspace threats.

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, priorities efficiently, or effectively consolidate resources. Lastly, NPPD needed to strengthen its communications and information sharing activities with international partners to effectively promote international incident response, exchange of cyber data with other nations, or the sharing of 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.[10]

Conclusion

DHS OIG completes significant audit, inspection, and investigative work to promote the economy, efficiency, effectiveness, and integrity of the Department's programs and operations. Our reports provide the Department Secretary and Congress with an objective assessment of the issues, and at the same time provide specific recommendations to correct deficiencies and improve the economy, efficiency, and effectiveness of the respective programs.

From April 1, 2012 through September 30, 2012, our audits resulted in questioned costs of over $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.

[9] DHS-OIG, *Transportation Security Administration Has Taken Steps To Address the Insider Threat But Challenges Remain* (OIG-12-120, September 2012).
[10] DHS-OIG, *DHS Can Strengthen Its International Cybersecurity Programs* (OIG-12-112, August 2012).

Our work, however, is only effective if the Department implements corrective actions timely to address deficiencies and weaknesses. Doing so will help to ensure that the Department exercises proper stewardship of Federal resources.

Mr. Chairman, this concludes my prepared statement. I appreciate your time and attention and welcome any questions from you or members of the Committee.

Biography -- Deputy Inspector General Charles K. Edwards

Charles K. Edwards resumed his position of record as Deputy Inspector General on January 4, 2013, and remains as head of DHS OIG, a role he first attained when he was named Acting Inspector General on February 27, 2011.

Mr. Edwards has more than 22 years of experience in the Federal government and has held leadership positions at several agencies, including the Transportation Security Administration, the United States Postal Service Office of Inspector General, and the United States Postal Service.

He has received numerous awards for his outstanding contributions to the Federal and law enforcement communities, as well as awards for excellence and distinguished achievement from individual Offices of Inspector General and the Federal Inspector General Community as a whole.

Mr. Edwards is a graduate of Loyola College in Maryland, with a double Masters Degree in Electrical Engineering and Computer Engineering. He also holds a Federal Chief Information Officer Certificate and Master's Certificate in Information Technology Project Management from Carnegie Mellon University. In addition, Mr. Edwards is certified as a Project Management Professional.