STATEMENT OF CHARLES K. EDWARDS

ACTING INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS AND MANAGEMENT

COMMITTEE ON HOMELAND SECURITY

U.S. HOUSE OF REPRESENTATIVES

CONCERNING

"ELIMINATING WASTE, FRAUD, ABUSE AND DUPLICATION IN THE DEPARTMENT OF HOMELAND SECURITY

MARCH 8, 2012

Good morning Chairman McCaul, Ranking Member Keating, and distinguished members of the Committee:

I am Charles K. Edwards, Acting Inspector General of the Department of Homeland Security (DHS). Thank you for the opportunity to testify today on our ongoing efforts to identify and eliminate waste, fraud, abuse, and duplication in the Department.

As you know, the DHS Office of Inspector General (OIG) was established in January 2003 by the *Homeland Security Act of 2002* by amendment to the *Inspector General Act of 1978.* The DHS OIG seeks to promote economy, efficiency, and effectiveness in DHS programs and operations and reports directly to both the DHS Secretary and the Congress. We fulfill our mission primarily by issuing audit, inspection, and investigative reports that include recommendations for corrective action, and by referring cases to the United States Attorney General for prosecution.

I would like to begin by noting the strides DHS has taken toward building a cohesive agency that addresses its key mission objectives to protect our borders, improve our response to manmade and natural threats, and implement transportation and trade security. DHS, by virtue of the breadth and importance of its mission, the scope of its activities, and the number of employees, must overcome some especially difficult challenges.

Each year we publish a report on the most significant management challenges facing the Department including acquisition management, grants management, and transportation security. Today, my testimony will highlight important issues in those three areas.

I am pleased to report that not only did DHS and its components concur with majority of our recommendations in these areas; in most cases they are already taking steps to implement these recommendations.

Acquisition Management

The Department continues to streamline its management of acquisitions, but is still challenged by their magnitude and complexity. Good acquisition management is critical to the Department's efforts to prevent fraud, waste and abuse, particularly good acquisition planning and adequate oversight and controls, as well as best practices such as strategic sourcing of common equipment. I would like to highlight four of our 2011 reports focusing on these issues.

In our report, *U.S. Customs and Border Protection's Management of the Purchase and Storage of Steel in Support of the Secure Border Initiative (OIG-12-05)*, we determined that U.S. Customs and Border Protection (CBP) did not effectively manage the purchase and storage of steel in support of the Secure Border Initiative. Since 2008, CBP spent approximately $1.2 billion to construct physical barriers along the southwest border as part of this initiative. About $310 million of the cost was to purchase and store steel in support of fence construction. CBP purchased steel based on an estimate before legally acquiring land or meeting international treaty obligations. In addition, it did not provide effective contract oversight during the project: it paid invoices late, did not reconcile invoices with receiving documents, and did not perform a

thorough review of the contractor's selection of a higher-priced subcontractor or document the reasons for its approval of the subcontractor. As a result, CBP purchased more steel than needed, incurred additional storage costs, paid interest on late payments, and approved a higher-priced subcontractor, with additional expenditures of about $69 million that could have been put to better use.

CBP did not efficiently plan the purchase and storage of steel for the Supply and Supply Chain Management (SSCM) task order. It purchased 27,557 tons of extra steel, with a value of about $44 million, which remained in storage at the end of the task order. Additionally, CBP did not obtain necessary approval to build all planned fence segments before acquiring the steel. In September 2009, CBP purchased 34 tons of steel for $23,000, even though it had significant quantities of the same steel already in storage. CBP was not proactive and did not efficiently plan for the storage of steel remaining from the task order. Instead of moving the extra steel to a cost-efficient location, CBP extended the original contract and awarded a supplemental storage contract. CBP's decision to extend the storage contracts for 2 years resulted in $9.8 million in avoidable storage costs.

CBP did not reconcile or promptly pay invoices from the SSCM task order. The cost of the task order increased because CBP paid invoices late, which resulted in late payment interest charges. Furthermore, CBP could not guarantee the government received what it paid for under the task order. CBP did not have policies and procedures for submitting and reviewing invoices. There was no clear guidance on the proper office to route invoices to, no timeline for the review process, and no notification process to remind offices of invoices coming due.

CBP did not perform a thorough review of the consent to subcontract documentation and did not document the reasons for its approval of the higher-price subcontractor. Its approval of a subcontractor may have added about $13.5 million to the project. The DHS Office of the Chief Procurement Officer recognized the importance of component oversight of subcontractor selection and issued an acquisition alert in April 2011 to DHS heads of contracting activities.

We noted that CBP should ensure it applied lessons learned from this project to future projects. To that end, we made five recommendations to improve CBP's management of future fence construction and contract oversight. CBP concurred with four recommendations, and DHS proposed an alternative to the fifth recommendation that met the intent of that recommendation. CBP was acting to implement the recommendations.

In *DHS Oversight of Component Acquisition Programs (OIG-11-71)*, we reported that DHS generally had management oversight and controls over components' acquisition programs, but needed to further refine some policies and strengthen oversight in some areas.

The Department had made progress in its acquisition oversight processes and controls by implementing a revised *Acquisition Management Directive (Directive 102-01)* and accompanying *Acquisition Instruction Guidebook (102-01-001).* The directive and guidebook addressed many previously identified oversight and control problems related to acquisition management. However, the guidance needed further refining to provide additional details and improve controls in some areas.

The Department had not fully defined for its components what constituted an acquisition program, and had not developed consistent guidance for reporting the three levels of acquisition programs in its standard reporting system. Components were not completing and reporting all key information into the next Generation Periodic Reporting System (nPRS), and were thus distorting the acquisition portfolio position through inconsistent reporting of programs. In July 2010, data from nPRS showed progress in entering level 3 acquisition program components, but the system still only reflected half the total number of level 3 programs that components were reporting outside nPRS. By mandating use of nPRS for all acquisition programs, the Department would have visibility into components' acquisition programs and could provide better oversight of its acquisition portfolio.

The Department did not ensure that components were using all available acquisition tools, including nPRS and the Strategic Sourcing Program Office (SSPO). Component personnel had developed or were developing their own data tracking systems because the Department had not consistently mandated use of nPRS or its tools. The Department also did not ensure that components were using the SSPO to manage acquisition programs, which would have created transparency and efficiency in their acquisition programs. As a result, components may have awarded contracts without considering the SSPO, and the Department may have incurred increased costs for procurements. In addition, components may have conducted duplicative market research for procurements that had already been done by the SSPO. The Department should ensure components were at least considering the use of the SSPO before awarding contracts.

DHS did not ensure that all components had developed adequate policies and procedures to manage and oversee acquisition programs. The Department's Acquisition Management Directive 102-01 states that components are authorized to establish internal acquisition processes and procedures consistent with the Directive. However, not all components had created such processes and procedures. Others had created program management offices to manage simple procurements, were not properly reporting programs into the standard system, or were not applying strategic sourcing strategies to support program development. The Department had not ensured the adequacy of the processes and procedures that components developed. As a result, some components unnecessarily created acquisition programs, which potentially increased administrative costs without adding value to the programs. In addition, the Department did not always know what is in its acquisition portfolio.

We made four recommendations to the Chief Procurement Officer to strengthen the Department's management oversight and controls over component acquisition programs, including requiring reporting of acquisitions in nPRS, implementing a plan of action or deadline to finalize acquisition management policies and procedures, and requiring components to consider using the SSPO and other resources in planning acquisitions. The Chief Procurement Officer agreed with our recommendations, and DHS initiated corrective actions.

The report, *DHS Continues to Face Challenges in the Implementation of Its OneNet Project (OIG-11-116)*, presented the results of our audit of DHS' efforts to consolidate its components' networks into a single wide area network, OneNet. In 2005, DHS began to consolidate and

transform existing individual component networks into a single, world-class information technology (IT) infrastructure. As part of an IT Infrastructure Transformation Program, OneNet's goal was to provide a reliable, cost-effective IT platform for data sharing among components in support of cross-organizational missions.

DHS had made some progress toward consolidating the existing components' IT infrastructures into OneNet. The Department had established a centralized Network Operations Center/Security Operations Center to manage and oversee OneNet and to monitor, detect, and respond to IT security incidents. All but three components were signing memorandums of agreement with CBP to obtain network and security services; as the OneNet steward, CBP had elected not to prepare an agreement. All components had converted their sites to Multiple Protocol Label Switching architecture to read and access audit trails captured on firewall and intrusion detection devices. The Department had also established a redundant trusted Internet connection (RTIC) to provide a redundant network infrastructure and essential OneNet services (e.g., Internet, extranet, and application hosting) to all DHS components.

At the time of our review, the Department needed to improve its implementation of OneNet. DHS needed to establish component connections (peering) to OneNet and ensure that all components transitioned to the RTIC. At the time of our audit, only two components had peered all their sites to OneNet; the remaining seven components identified the lack of Policy Enforcement Points (PEP), which support controlled cross-communication among component Trust Zones, as the primary reason for their delayed transition to OneNet. DHS components had established different and unique levels of IT security policies, as well as different PEPs, to enforce these policies. Not all DHS components had completely transitioned to the RTIC. As of February 2011, two components had completed their transition. Three of the remaining seven components had signed waivers with extension dates until 2012 to defer their transition to the RTIC. Finally, DHS had not completed required OneNet management documents, such as the Concept of Operations, which describes how to use desired capabilities to carry out operations. Three components did not have required interconnection security agreements, and three other such agreements had expired.

We recommended that the DHS Chief Information Officer complete the transition and connection (peering) of components and develop and implement key planning documents, network service agreements, and interconnection security agreements for OneNet. DHS generally agreed with our findings and recommendations.

In *DHS Department-wide Management of Detection Equipment (OIG 11-47)*, we found the Department could better manage acquisition of detection equipment by developing processes to standardize equipment purchases and identifying common mission requirements among components. DHS had eight different procurement offices purchasing detection equipment and did not have a process to facilitate strategic sourcing. The Department was using multiple models to meet similar missions, and thus, was incurring higher administrative, logistical support, and maintenance costs. We identified about $170 million worth of small x-ray machines, metal detectors, and personal and hand-held radiation detectors that DHS could acquire through strategic sourcing strategies. To strategically source, DHS would need to standardize purchases of explosive, metal, and radiation detection equipment; and identify

common mission requirements among components. Limiting the models and types of equipment would increase procurement, maintenance, and personnel efficiencies.

Components were also maintaining separate inventories, and the inventory systems were not based on standard inventory data elements and standard nomenclature for similar detection equipment. Without a dictionary of common data elements and nomenclature, the Department did not have timely visibility over on-hand balances of equipment and could not be sure inventory data was complete and accurate.

We made two recommendations to the Deputy Under Secretary for Management. First, we recommended that DHS establish a standard data dictionary, consolidate data descriptions, and make sure components use consistent inventory terms; second, we recommended that DHS re-establish a Joint Requirements Council to identify cross-cutting opportunities and common requirements. DHS concurred with both recommendations and reported it was developing standard data elements to manage its inventory accounts and was planning to revive the Joint Requirements Council.

Disaster Assistance Fraud

The report, *Assessment of FEMA's Fraud Prevention Efforts (OIG-11-84)*, included results of our review of FEMA's Individuals and Households Program (IHP), through which the agency quickly disburses billions of dollars to disaster survivors. The program's vulnerability to fraud, waste, and abuse requires FEMA to implement procedures designed to ensure assistance is provided in proper amounts and only to eligible recipients. While FEMA had made progress in preventing fraudulent losses of federal funds, challenges remained in reporting and identifying fraud; increasing fraud prevention awareness; developing and maintaining proper internal controls; and recouping improper disaster assistance payments.

The report highlighted the fact that FEMA had not established an environment in which employees understand that fraud prevention is integral to the agency's mission. This is partially caused by FEMA not training disaster assistance employees how to prevent and detect fraud, waste, and abuse. Rather, FEMA offered non-mandatory ad hoc training to those employees who wanted to take the training. FEMA's leaders must continually demonstrate the importance of fiscal responsibility and program integrity. Mandating fraud prevention training for all employees would increase the agency's attention to fraud prevention and deterrence.

The agency had improved its internal controls since hurricanes Katrina and Rita. However, OIG and Government Accountability Office reviews, as well as agency assessments, continued to identify needed improvements in internal controls over its assistance programs. For example, in September 2009, we reported that FEMA substantially improved internal control weaknesses that existed during hurricanes Katrina and Rita. While these changes resulted in fewer instances of payments made to registrations with duplicate and invalid key data, FEMA does not always use all of its validity checks for key registration data. Consequently, FEMA continued to make improper disaster assistance payments that should have been avoided. FEMA needs to consistently apply its existing business rules, and monitor payment activities to update its internal controls when it indentifies new vulnerabilities.

The goal of the Fraud Prevention and Investigation Branch (FPIB) is to assist in identifying, mitigating, and preventing fraud in FEMA programs through fraud awareness training and, in partnership with DHS, recoupment of losses. FEMA should issue a management directive establishing FPIB as an agency-wide entity with authority to review all FEMA-funded programs and recommend improvements to internal controls to deter and prevent fraud, waste, and abuse. FEMA needs also to provide additional staffing to enable the FPIB to achieve that goal and adopt measures used by the Recovery Accountability and Transparency Board, such as the fraud-mapping tool, to foster accountability and transparency of FEMA programs and improve internal controls. Finally, FPIB's visibility would be enhanced if it reported directly to the FEMA Office of the Administrator, or one of his direct reports.

Transportation Security

Transportation security is one of the critical missions for which DHS was created. Since its inception, the Department has invested considerable resources to establish a secure transportation environment, particularly at our nation's airports. We have audited many of the layers of security established or overseen by TSA. One of our recent reports, *TSA's Oversight of the Airport Badging Process Needs Improvement*, examined TSA's controls over the issuance of airport badges to individuals.

Individuals who pose threats may obtain airport badges and gain access to secured airport areas, endangering the safety of airport workers, passengers, and aircraft. We identified badges issued to individuals with one or more omissions or inaccuracies in key applicant data used for vetting. For example, badges were issued to individuals without a complete security threat assessment (STA). Individuals were not always properly vetted, and badges were issued without the required information such as STA status, birthdate, and birthplace. Airport operators and local TSA officials were not fully aware of the details of the complex vetting process and the ramifications of entering inaccurate biographical data.

TSA had designed and implemented only limited oversight of the badge application process. Specifically, the agency did not ensure that airport operators had quality assurance procedures to safeguard the completeness and accuracy of the data used for vetting. Despite its reliance on designated airport operator employees, TSA did not always ensure that airports were properly training these employees. Only one airport had a formalized training program focused on airport operator employees' duties and responsibilities. TSA also did not ensure that airport operator employees were using available tools to perform their assigned duties.

In addition, TSA did not require its Inspectors to verify airport data during interviews. TSA Inspectors reviewed the airport badging process during inspections; however, this limited coverage did not ensure that vetting information was complete and accurate. Inspectors did not always have direct access to the Transportation Security Clearinghouse database and were not required to compare or cross-reference records. Therefore, inspections of badging office records may have been insufficient to determine the airports' level of compliance with vetting process requirements. Direct access to clearinghouse data would enable Inspectors to verify records for approved STAs in a timely manner and take immediate corrective action if necessary.

TSA did not require airports to conduct recurrent Criminal History Records Checks (CHRC) to ensure that badge holders maintained their reputable status. According to airport and TSA officials, these checks should be conducted on a recurrent basis. These officials also indicated the self-reporting policy was ineffective because most employees would not report themselves for fear of losing their job. Some airports were proactive in mitigating risk in the CHRC process. According to TSA officials, the agency recognized the need for more frequent criminal checks. The Transportation Threat Assessment and Credentialing office, in cooperation with the agency's Office of Chief Council, was exploring implementation of a requirement to conduct recurrent CHRCs.

Some sites we visited had best practices that could be implemented at other airports to ensure authenticity of documentation and data accuracy. In addition, in response to our preliminary findings, the Airports Council International-North America established a task force of its member airports to identify and evaluate best practices for airport identification badging. Some practices included conducting badging application audits to identify common errors to incorporate into training classes, providing advanced training on fraudulent document identification and document handling procedures, establishing checks to prevent duplicate records, and establishing a quality control process to review applicant information before it is submitted for an STA.

We presented our findings to the airport operators, local TSA officials, and Inspectors. Our analysis generated 101 updates, which airport operators sent to the Transportation Security Clearinghouse. We made recommendations to establish and implement quality assurance procedures for the badging process, ensure that airport operator employees receive proper training and tools to perform their assigned duties, require independent verification of approved applications, provide real time reports on active badge holders, and conduct recurrent CHRCs. TSA concurred with all but one recommendation—on real time reporting—with which it partially concurred.

In closing, I would like to commend the Department for acting quickly on our recommendations in an effort to improve its operations and performance. The Office of Inspector General remains committed to performing audits and inspections, identifying issues, and making recommendations to assist DHS in carrying out its mission effectively and efficiently.

Mr. Chairman, this concludes my prepared statement. Thank you for the opportunity to testify, and I welcome any questions from you or Members of the Committee.