STATEMENT OF CHARLES EDWARDS

DEPUTY INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

U.S. HOUSE OF REPRESENTATIVES

CONCERNING

DHS INFORMATION TECHNOLOGY: HOW EFFECTIVELY HAS DHS HARNESSED IT TO SECURE OUR BORDERS AND UPHOLD IMMIGRATION LAWS?

MARCH 19, 2013

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss DHS' information technology (IT) issues. My testimony today will address the predominant IT management issues we have reported on over the past two years.

The majority of information that I will provide is contained in our reports, *Customs and Border Protection Information Technology Management: Strengths and Challenges (OIG-12-95), DHS Information Technology Management Has Improved, But Challenges Remain (OIG-12-82), U.S. Citizenship and Immigration Services' Progress in Transformation (OIG-12-12), Coast Guard Has Taken Steps To Strengthen Information Technology Management, but Challenges Remain (OIG-11-108), Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology (OIG-11-69), and U.S. Secret Service's Information Technology Modernization Effort (OIG-11-56).* I will also provide an update on the progress made by DHS on implementing some of the report recommendations.

DHS budgets over $6 billion a year for its IT. This represents nearly 15 percent of the DHS overall budget. The 22 component agencies that currently make up DHS rely extensively on IT to perform a wide range of mission operations, including counterterrorism, border security, and immigration benefits processing, among others. Given the size and significance of DHS' IT investments, effective management of department-wide IT expenditures is critical.

DHS' IT Management Oversight

In the past, we identified the need for the Department's Chief Information Officer (CIO) to have greater authority to become a more effective steward of IT funds.[1] The Department has since strengthened the CIO's responsibilities for oversight and centralized management of IT, which has helped provide the authority for leading component CIOs toward a more unified IT direction. Specifically, we reported in May 2012 that the DHS Office of the CIO has improved oversight of IT programs and key IT management functions, such as acquisition and portfolio reviews, to improve CIO decision making.[2] As a result, the DHS CIO has better visibility of department-wide IT programs and assets thus enabling the CIO to identify opportunities for reducing costs and duplication across the Department's IT environment.

In the same report, we concluded that DHS had further defined the CIO's authority and responsibility. For example, the DHS Deputy Secretary issued a memorandum in May 2011, which directed the CIO to take a greater role in the review and execution of all IT infrastructure investments.[3] The expansion of DHS CIO authority was due in part to the Federal CIO's IT reform plan, which requires agency CIOs to implement initiatives to improve management of large-scale IT programs.[4] Additionally, Office of Management and Budget Memorandum M-

[1] *Improvements Needed to DHS' Information Technology Management Structure* (OIG-04-30, July 2004). *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG-08-91, September 2008).
[2] *DHS Information Technology Management Has Improved, But Challenges Remain* (OIG-12-82, May 2012).
[3] DHS Deputy Secretary, *Information Technology Efficiency*, May 5, 2011.
[4] The *25 Point Implementation Plan To Reform Federal Information Technology Management*, December 9, 2010.

11-29, *Chief Information Officer Authorities*, states that agency CIOs must drive the investment review process for IT investments. To formalize this guidance, the DHS Undersecretary for Management began an effort to update the Delegation of Authority for the DHS CIO, which included oversight of the Department's IT programs.

The CIO has increased oversight of department-wide IT programs and investments by conducting annual IT program reviews and in-depth reviews of selected IT programs. These reviews enable the CIO to make strategic recommendations for reducing costs and duplication across the Department's IT environment. For example, the DHS CIO issued 90 recommendations to the Deputy Secretary for the 2013 budget year for 81 IT investments continue as planned, eight investments be continued but modified, and one be suspended. The CIO also made program specific recommendations, such as to reinstate $10 million in funding per year for the Customs and Border Protection (CBP) Traveler Enforcement Compliance System Modernization in order to prevent further schedule delays, as well as a recommendation that the Federal Emergency Management Agency (FEMA) suspend work on its National Flood Insurance Program Information Technology Systems and Services until business requirements were better defined.

In addition, the DHS CIO has increased oversight of IT software, hardware, and infrastructure purchases through the IT acquisitions review process. The volume of IT acquisition reviews has increased from 243 in FY 2007 to 387 in FY 2011. The number of approvals for IT acquisition requests has increased from 129 in FY 2007 to 311 in FY 2011. These reviews have increased the DHS CIO's ability to verify compliance with technical standards and to ensure program and project alignment with department-wide IT policy, standards, objectives, and goals.

The Department has also achieved infrastructure integration milestones through data center and network consolidation. Specifically, the Office of the CIO (OCIO) continues its efforts to consolidate data centers across the Department, integrate disparate component networks into a single DHS network, and create centralized email and collaboration services to improve information sharing. As of November 2011, DHS headquarters, FEMA, the Transportation Security Administration (TSA), and CBP had migrated applications from eight sites to one DHS enterprise data center. Additionally, DHS has established an enterprise network, OneNet, as well as a primary and secondary network operations center and security operations center. The OCIO has also begun offering centralized IT services housed at the two enterprise data centers, such as email and Microsoft SharePoint, to achieve economic savings through consolidation. Some components are already realizing cost savings from the data center consolidation and DHS enterprise service offerings.

Finally, the Department matured key IT management functions, such as strategic planning, Capital Planning and Investment Control (CPIC), enterprise architecture, and portfolio management. For example, the OCIO developed an IT strategic plan for FY 2011–2015. In addition, the DHS OCIO has continued to execute its CPIC process effectively, which is DHS' primary process for making decisions about the systems in which the Department should invest. The OCIO has also continued to execute department-wide enterprise architecture efforts, such as the development of a Homeland Security Enterprise Architecture and specific segment architectures, which provide the CIO with a foundation for making better informed decisions.

Finally, the DHS Portfolio Management process, which establishes portfolios based on DHS' mission areas and business functions, helps the OCIO to align IT investments with portfolios and identify redundancies or gaps. Over the past two years the DHS OCIO has begun conducting an annual portfolio analysis to align IT investments to its 13 existing portfolios and identify redundancies or gaps. At the time of our audit, the OCIO had aligned more than 650 IT investments with the 13 portfolios.

Major Challenges

Although DHS has made significant progress in improving IT management functions, challenges remain for CIO involvement in component IT budget planning. For example, the DHS CIO conducts a review of all components' IT budgets as part of the DHS IT budget formulation process, which provides opportunity to confirm that component plans are in line with departmental priorities. However, the CIO is not involved during the component IT budget planning process when initial planning activities are taking place. As such, the CIO IT budget reviews do not directly affect the amount of funding components receive, meaning components can obtain funding for IT investments regardless of the decisions made during the budget review process. For example, a review of one component's IT budget revealed a funding request for approximately $6 million to improve IT infrastructure. Yet, the OCIO had requested $91 million from the component for data center migration costs for the same budget year, highlighting a discrepancy in funding plans.

To address this issue we recommended that the Deputy Under Secretary for Management assign the DHS CIO centralized control over the Department's IT budget planning process to review, guide, and approve IT investments. Since this recommendation was made, the DHS CIO has been delegated the authority to review and approve IT budgets for delivering and maintaining enterprise IT solutions and mission IT systems and services throughout the Department in coordination with the DHS CFO. The recommendation was closed in September 2012.

Component-Specific Challenges

Insufficient IT management practices, need for CIO IT budget authority, fragmented and aging IT infrastructures, and inadequate governance mechanisms have been long-standing issues for several DHS components.

Component IT Management Practices Need Improvement

Although DHS and its components have made progress establishing effective IT management practices, several DHS components have not fully implemented key IT management functions needed to guide agency-wide IT programs. For example, in June 2012 we reported that CBP had developed an enterprise architecture to align with the Department's architecture and guide CBP's IT environment.[5] However, the Office of IT had not yet developed a target "To-Be" business

[5] *CBP Information Technology Management: Strengths and Challenges* (OIG-12-95).

architecture to analyze business processes. Without a complete view of CBP's target enterprise architecture, the CIO faces increased risks to efforts to modernize the way OIT provides support to CBP. We recommended the CBP OIT provide the necessary resources to complete required enterprise architecture activities.

Similarly, we reported in April of 2011 that FEMA had not yet completed its enterprise architecture. Specifically, the agency had not completed efforts to document its business functions, information resources, and IT systems as part of its baseline enterprise architecture. [6] Also, the IT architecture remained undocumented for many program areas and the standards on the OCIOs website were at least two years out of date. We also determined that FEMA did not have a comprehensive IT strategic plan with clearly defined goals and objectives or guidance for program office initiatives. Without these critical elements in place, FEMA is challenged to establish an effective approach to modernize its information technology infrastructure and systems. We recommended FEMA complete and implement an enterprise architecture and develop a comprehensive IT strategic plan. Each of these recommendations were closed in January 2013 when FEMA produced evidence of a completed baseline architecture and an updated IT Strategic Plan.

Likewise, we reported in March of 2011 that the United States Secret Service (USSS) had not updated its IT Strategic Plan since 2006.[7] As a result, its plan was not sufficient to address its system weaknesses or integrate with DHS' technology direction. For example, the plan did not describe how the USSS will leverage specific DHS enterprise-wide solutions such as DHS Consolidated Data Centers and OneNet. Additionally the IT Strategic Plan did not accurately reflect Information Integration and Transformation Program activities such as planned upgrades to technology platforms. We recommended that the Deputy Director, USSS create effective planning documentation.

Component CIOs Need Additional Budget Authority and Oversight

Most of the major component CIOs lack IT budget authority and oversight of technology spending across programs and activities within their agency. For example, in our June 2012 review of CBP we found that the CIO did not have full oversight of IT spending across all programs and activities within CBP.[8] Specifically, CBP component offices submit IT spending requests that were processed by procurement without going through the CIO's IT acquisition review process, thus increasing the risk of security issues or enterprise alignment challenges. Likewise, in April 2011 we reported that FEMA's program offices and regional offices continue to develop IT systems independent of the OCIO due in part to decentralized IT budget and acquisition practices. Specifically, the manner in which IT programs are funded and developed within FEMA hindered the OCIO's efforts to establish a complete inventory and manage IT capital planning and investment. For example, during FY 2010, FEMA spent $391 million for agency-wide IT needs, but the OCIO accounted for only 29 percent of total spending. We recommended the FEMA CIO establish an agency-wide IT budget planning process to include

[6] *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology* (OIG-11-69).
[7] *U.S. Secret Service's Information Technology Modernization Effort* (OIG-11-56).
[8] *CBP Information Technology Management: Strengths and Challenges* (OIG-12-95).

all FEMA program technology initiatives and requirements.

In September 2011, we reported that the United States Coast Guard (USCG) CIO had limited authority over IT assets and spending.[9] Specifically, the CIO does not have sufficient oversight of IT spending by field units. Without this authority, the CIO cannot fully ensure that the Coast Guard IT environment is functioning effectively and efficiently. We recommended that Coast Guard Chief of Staff transition IT personnel and oversight of field IT spending under the CIO. Likewise, in our March 2011 review of USSS[10] we determined that the USSS did not position its CIO with the necessary authority to review and approve IT investments. Specifically, the CIO was not a member of the Director's management team and therefore does not play a significant role in overseeing IT systems development and acquisition efforts. We recommended the Deputy Director, USSS provide the CIO with agency-wide IT budget and investment review authority to ensure that IT initiatives and decisions support accomplishment of the USSS and department-wide mission objectives.

Outdated IT Does Not Effectively Support Component's Missions

Component CIOs are challenged to ensure that the IT environment fully supports its agencies mission needs. Commonly, interoperability and functionality of component's aging technology infrastructures have not been sufficient to support mission activities. For example, in June 2012 we reported that the CBP Office of IT (OIT) faced challenges with system availability, including periodic outages of critical security systems.[11] Systems outages have occurred in part because of aging infrastructure, which has not been updated as required because of funding reductions. In addition, the interoperability and integration of the IT infrastructure were not sufficient to support CBP mission activities fully, due to lengthy requirements gathering and technology insertion processes. As a result, staff created workarounds and employed alternative solutions, including assigning agents to perform duplicative data entry—instead of enforcement duties in the field—and operating stand-alone, non-approved IT. We recommended the CBP CIO develop a funding strategy for the replacement of outdated infrastructure. As of February 2013, the CBP OIT was continuing to assess the needs across CBP to present additional requirements for funding consideration and prioritization against all other CBP priorities.

Also, we reported in September 2011 that Coast Guard systems and infrastructure did not fully meet mission needs due to aging infrastructure that is difficult to support, and stovepiped system development.[12] Specifically, Coast Guard field personnel do not have sufficient network availability, the aging financial system is unreliable, and command center and partner agency systems are not sufficiently integrated. As a result, field personnel rely on inefficient work-arounds, such as having to enter the same information twice, to accomplish their mission. We recommended the Coast Guard CIO address the IT systems and infrastructure needs by implementing a plan to ensure system redundancy to meet availability requirements, implement a

[9] *Coast Guard Has Taken Steps To Strengthen Information Technology Management, but Challenges Remain* (OIG-11-108).
[10] *U.S. Secret Service's Information Technology Modernization Effort* (OIG-11-56).
[11] *CBP Information Technology Management: Strengths and Challenges* (OIG-12-95).
[12] *Coast Guard Has Taken Steps To Strengthen Information Technology Management, but Challenges Remain* (OIG-11-108).

strategy to improve ease of use and availability of the financial systems, and ensure that new tools address requirements for improved integration. Since that time, the recommendation to ensure that new tools address requirements for improved integration was closed in April 2012.

In April 2011, we reported that FEMA's systems were not integrated, did not meet user requirements, and did not provide the information technology capabilities agency personnel and its external partners needed to carry out disaster response and recovery operations in a timely or effective manner.[13] Specifically, limited progress had been made in modernizing the agency's critical mission support systems due to uncertainty of department-wide consolidation plans. As a result, FEMA's legacy systems were not able to effectively support disaster response functions in a timely and effective manner. As a result, FEMA personnel were using paper forms and relying on manual data entry to process grants. These manual work-arounds may suffice during minor events; however, they may not sustain the increased workload and level of information sharing required to support major disasters. We recommended the FEMA CIO establish a consolidated modernization approach for FEMA's mission-critical IT systems, to include DHS plans for integrated asset management, financial, and acquisition solutions. As of December 2012, FEMA had included modernization plans in its 2012 IT Strategic Operations Plan; however, the recommendation remains open until the OCIO develops a modernization approach for FEMA's mission-critical IT systems.

The United States Citizenship and Immigration Services (USCIS) faces similar challenges to establish an IT environment that can effectively support its mission needs. We reported in November 2011 that USCIS continued to rely on paper-based processes to support its mission, which made it difficult for USCIS to process immigration benefits efficiently, combat identity fraud, and provide other government agencies with the information required to identify criminals and possible terrorists quickly.[14] On any given day, USCIS processes 30,000 applications for immigration benefits. Yet, USCIS provides nearly all of its services using paper forms: customers submit paper application forms; USCIS adjudications officers determine whether an applicant is eligible for benefits by reviewing the paper documentation; and USCIS issues paper evidence of benefits. USCIS staff also must use automated and manual methods to conduct background checks on applicants. An enterprise-wide transformation program is underway to transition the agency from a paper-based operational environment to an account-based environment using electronic adjudication. However, implementation of the transformation has been delayed repeatedly over the past 8 years. We recommended that the Office of Transformation Coordination complete business and technology process documentation to provide the detail necessary to implement the transformation program effectively. Since that time, USCIS provided process documentation in July 2012 and the recommendation was closed.

Better IT Governance Needed for IT Modernization Efforts

Components implementing transformation efforts are hindered by insufficient governance and decision-making mechanisms to effectively direct agency-wide transformation program activities. In our March 2011 report, we found that the USSS did not implement an effective IT

[13] *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology* (OIG-11-69).
[14] *U.S. Citizenship and Immigration Services' Progress in Transformation* (OIG-12-12).

governance approach for its Information Integration and Transformation Program, which had an estimated cost of $1.5 billion.[15] Specifically, the agency did not have a formal department-level IT governance mechanism to provide integrated feedback and direction for the transformation program effort. Without a formal mechanism for integrated governance, the USSS reached out individually to DHS offices and received conflicting advice and did not sufficiently consider DHS enterprise-wide solutions. We recommended that the Deputy Director, USSS formalize an Executive Steering Committee and ensure that the Information Integration and Transformation Program is in alignment with the USSS and DHS strategic goals and objectives. Since that time, the USSS has provided updates on its ongoing efforts to implement an Executive Steering Committee which includes USSS Senior Management and DHS members from the offices of the CIO, the Chief Procurement Officer, and the Acquisition, Planning, and Management Directorate.

Likewise, our April 2011 review of USCIS Transformation concluded that USCIS' transformation governance structure did not promote timely and effective decision making.[16] Specifically, the governance structure was overly complex and required too many formal meetings and checkpoints for review, hindering decision making. We recommended that the Chief, Office of Transformation Coordination revise its current governance structure to enable more streamlined program decision making. Since that time, USCIS has continued to revise its governance structure to include a Transformation Executive Steering Committee and a Product Management Team.

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

[15] *U.S. Secret Service's Information Technology Modernization Effort* (OIG-11-56).
[16] *U.S. Citizenship and Immigration Services' Progress in Transformation* (OIG-12-12).