STATEMENT OF JAMES L. TAYLOR

DEPUTY INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON MANAGEMENT, ORGANIZATION, AND PROCUREMENT

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 15, 2009

Ms. Chairwoman and Members of the Subcommittee:

Thank you for the opportunity to appear before you on behalf of the Department of Homeland Security Office of Inspector General. My testimony today will focus on the progress in IT acquisition management DHS has made over the past several years, as well as several challenges the department and its components face going forward. Specifically, I will discuss our work related to the establishment of institutional and investment management capabilities for delivering major information technology (IT) system acquisitions programs at DHS.

The information that I will provide is contained in two reports we've issued on DHS and its components' IT management practices, *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG-08-91) and *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology* (OIG-09-90); as well as our annual *Major Management Challenges Facing the Department of Homeland Security (OIG-09-08).*

DHS Acquisition Management

Contracting for goods and services consumes nearly 40% of the department's annual budget and is critical to achieving its mission. Acquisition management is a complex process that involves much more than simply awarding a contract. It begins with identification of a mission need, the development of specific requirements, and a strategy to fulfill that need and meet those requirements while balancing cost, schedule, and performance. A successful acquisition process requires an effective acquisition management infrastructure and skilled professionals.

In our November, 2008 Major Management Challenges report, we rated the department's progress in four areas of acquisition management: organizational alignment and leadership; policies and processes; acquisition workforce; and knowledge management and information systems. In all these areas, we rated the department's progress as "Modest." While we identified some improvements, our reviews indicated that many of the critical success factors had not yet been met.

DHS' IT Investment Management Oversight

DHS spends over $6 billion a year for IT systems and infrastructure to support its mission. The department's component agencies rely extensively on information technology to perform mission operations, including immigration benefits processing, support for its security mission, the execution of response and recovery operations, human resources and financial management, and many others. Given the size and significance of DHS' IT investments, effective management of department-wide IT expenditures is critical.

The Clinger-Cohen Act requires that departments and agencies create a capital planning and investment control (CPIC) process to manage the risk and maximize the value of IT acquisitions. The CPIC process is intended to improve the allocation of resources to benefit the strategic needs of the department. As part of the CPIC process, agencies are required to submit business plans for IT investments to OMB demonstrating adequate planning. Through such efforts, in FY 2007, the 94 DHS programs on the management watch list were reduced to 18. In FY 2008, 53 programs were listed. Officials in the OCIO have sought to remove these programs from the list by working with the program managers through the CPIC Administrator's bimonthly meetings.

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] Most components have not yet achieved an integrated planning and investment management capability. More than 70% of the major DHS components had limited capital planning processes outside the existing OMB 300 process. However, some component CIOs said that they are creating a CPIC process to integrate with existing governance structures such as the Investment Review Board. For example, the ICE Investment Review Board resembles a CPIC group, incorporating major areas such as security, budget, and enterprise architecture. The ICE CIO said that this process has helped components leverage resources more effectively.

The department has strengthened the CIO's role for centralized management of IT, providing the CIO the authority to guide IT investments to ensure a unified IT direction across DHS components.

Additionally, the DHS CIO has gained greater authority over component-level IT budgets and oversight of IT acquisitions. This has resulted from the establishment of new policies and IT investment governance functions. For example, DHS management directive 0007.1, *Information Technology Integration and Management*, establishes the IT acquisition authorities and responsibilities of the DHS CIO, and is the principal document for leading, governing, integrating, and managing the department's IT. The directive also defines the department's IT acquisition review (ITAR) process.

Improvements to IT Acquisitions and Governance

Implementation of the ITAR process has increased the DHS CIO's ability to ensure program and project alignment with department-wide IT policy, standards, objectives, and goals. For example, it has enabled the DHS CIO to direct IT efforts toward the department's primary infrastructure goals, such as consolidating component network and data centers.

Additionally, the ITAR process has improved compliance with the DHS enterprise architecture, enabling the DHS CIO to direct IT efforts to align with the department's

[1] *Improvements Needed to DHS' Information Technology Management Structure* (OIG-04-30, July 2004).

target architecture goals. For example, the Transportation Security Administration (TSA) planned to create an E-authentication solution for its Alien Flight School Program. However, during the ITAR process, the Office of the CIO (OCIO) recognized that TSA's system needs could be met by using the solution that U.S. Immigration and Customs Enforcement (ICE) created for its Student Exchange Visitor Information System, thus preventing unnecessary duplication.

Component-level CIOs also have benefited from the ITAR process, which requires that component IT procurement requests be approved by the CIO before they are completed by the acquisitions office. Under this process, the TSA CIO identified opportunities to use more enterprise licenses for products, such as security software, and consolidated IT support contracts, resulting in cost savings.

The DHS CIO relies on a variety of IT investment governance structures and functions to ensure compliance with IT management policies and to promote centralized IT management, including the CIO Council, an Investment Review Board, an Enterprise Architecture Board, the Capital Planning and Investment Control process, and Portfolio Management process.

The DHS CIO Council sets the vision and strategy for the IT function and information resources. This council provides recommendations for the department IT strategic plan and establishes policies, processes, best practices, performance measures, and decision criteria for managing IT service delivery. According to several component CIOs, the council has improved component collaboration, productivity, and communication. The Investment Review Board is a governance body responsible for providing senior managers with visibility, oversight, and accountability for IT investments. The DHS CIO plays a major role in reviewing IT investments that reach the Investment Review Board. The Enterprise Architecture Board is an investment review mechanism that has improved department-wide IT management functions. The board's review ensures that IT investments align with the department's enterprise architecture and that sound IT investment approval recommendations are provided to the DHS CIO.

As discussed earlier, the CPIC process requires components to submit business cases for IT investments to demonstrate adequate planning. The business cases are reviewed for approval and progress based on the Office of Management and Budget's annual budget process. CPIC administrators from each component act as liaisons between the department and the component programs to aid the CPIC process. These administrators regularly review issues and identify process improvements. The DHS Portfolio Management process establishes portfolios based on DHS' mission areas, strategic goals, and objectives to align IT investments with DHS' strategic objectives. Operating these governance bodies and executing these processes require commitment and a significant amount of resources, including staff time.

Ongoing Challenges

Implementing the ITAR process has been challenging and we continue to identify problems with outdated or stove-piped systems, at times supporting inefficient business processes. Planning to modernize IT has been unfocused, often with inadequate requirements identification, analysis, and testing to support acquisition and deployment of the systems and other technologies needed to improve operations.

In 2007, only 57% of the department's estimated $5.6 billion IT budget was evaluated through the ITAR process. Department officials stated that there has been a lack of sufficient DHS CIO and component CIO staff to effectively execute the ITAR processes at the department and component levels. In 2004, around 75% of the federal positions within the OCIO were filled. By 2007, only 64% of the positions were filled.

Unable to obtain and keep fulltime, federal employees, the OCIO has depended heavily on contractor support. The number of contractors increased from 121 in 2004 to 550 in 2007. A combination of factors have contributed to the low staffing numbers, including the complex and lengthy hiring process that involves background checks for security clearances. Once OCIO positions are filled, employees become "burned out" from working long hours and end up leaving for positions in the private sector.

To address its staffing issues, we recommended that the DHS CIO improve the DHS OCIO Staffing Plan to include specific actions and milestones for recruiting and retaining fulltime employees. We closed this recommendation in June 2009 based on the department's development of a revised staffing plan that detailed plans to increase federal positions and to augment overall staff by 236 throughout the OCIO by 2011.

Agencywide IT Infrastructure Initiatives

Even with these improvements, the department will continue to face significant challenges as it attempts to create a unified IT infrastructure for effective integration and agencywide management of IT assets and programs. Toward that end, DHS has several initiatives underway to improve IT operations and reduce costs. One such program is the development of an enterprise-wide IT disaster recovery program to ensure that the department's operations can continue uninterrupted should its IT systems fail. We reported in April 2009 that DHS had made progress in implementing a disaster recovery program by allocating funds to establish two new data centers.[2] However, we noted that more work was needed to ensure the new data centers were fully capable of meeting the department's significant IT disaster recovery needs.

Another major IT challenge for the DHS CIO is OneNet, an initiative aimed at consolidating existing IT infrastructures into a wide area network. DHS began work on OneNet in 2005, and envisions it will provide the components with secure data, voice, video, tactical radio, and satellite communications between internal and external DHS resources. We recently reported that DHS has taken various steps to consolidate existing infrastructures into OneNet, but faces challenges in completing its OneNet

[2] *DHS' Progress In Disaster Recovery Planning for Information Systems* (OIG-09-60, April 2009).

implementation.[3] Specifically, we reported that DHS is experiencing delays in meeting its scheduled completion date, and that some components are reluctant to migrate to OneNet, have insisted on maintaining their own Internet gateways, and are hesitant to use DHS Trusted Internet Connection (TIC) services. As a result, DHS may not be able to reach its ultimate goal of consolidating and modernizing its existing infrastructures and achieve cost savings.

Component IT Management

Although improvements have been made, component CIOs also face significant challenges in their efforts to improve IT management, budgeting, planning, and investment. Because programs are often funded through direct appropriations or other sources, investment decisions may reside outside of the component CIO's purview. In these cases, offices and divisions maintain separate budgets that are independent of the CIO. Insufficient staff, ineffective IT budget controls, and fragmented IT management have been long-standing issues for several DHS components. For example:

U.S. Citizenship and Immigration Services (USCIS)

The USCIS CIO has been challenged to enforce compliance with component-level IT system development control mechanisms for the past several years. In January 2005, USCIS developed a transformation strategy that discussed the business requirements and vision for modernizing IT to meet mission needs. In September 2005, we reported that USCIS' IT environment is inadequate to effectively support immigration benefits processing.[4] Specifically, USCIS uses multiple, disparate information systems that are difficult to use and do not adequately share information, resulting in data integrity problems. The lack of a fully integrated IT environment has forced employees to spend time tracking the location of paper files as they are transferred among and within USCIS offices numerous times over their life cycle.

In November 2006, we reported on the results of a follow-up audit of USCIS' transformation program.[5] We noted that although USCIS had taken steps to address the recommendations in our 2005 report, the component had yet to finalize its transformation implementation approach. Subsequently, we reported in July 2009 that the large-scale USCIS transformation program is being managed outside of the CIO's Office of Information Technology.[6] The CIO identified the autonomy of the USCIS transformation program IT efforts and the program's exemption from normal USCIS controls as an emerging internal control deficiency. In addition, we reported that the continuation of decentralized, fragmented IT program efforts has led to a growing

[3] *Improved Management and Stronger Leadership are Essential to Complete the OneNet Implementation* (OIG-09-98, September 2009).
[4] *USCIS Faces Challenges in Modernizing Information Technology* (OIG-05-41, September 2005).
[5] *U.S. Citizenship and Immigration Services' Progress in Modernizing Information* Technology (OIG-07-11, November 2006).
[6] *U.S Citizenship and Immigration Services' Progress in Modernizing Information Technology* (OIG-09-90, July 2009).

number of local systems that are beyond the USCIS CIO's current budget or staffing level to manage effectively. Although the total number of locally-funded IT systems is unknown, USCIS field offices have reported thousands of applications were developed "in-house."

We concluded that transformation will be critical to support the agency's current workload, address the ongoing backlog, and prepare for future increases in demand for immigration benefits processing. Among other things, we recommended that the Acting Deputy Director provide the CIO agency-wide budget and investment review authority for all USCIS IT initiatives and system development efforts.

Transportation Security Administration (TSA)

The TSA CIO faces major challenges in managing and applying IT effectively in support of TSA's security mission. We reported in October 2007 that TSA strengthened its IT governance and acquisition processes.[7] However, technology investments were being managed in a decentralized fashion. Further we reported that TSA established an acquisition process and supporting governance structure, but has not instituted mechanisms for consistent oversight of agency-wide IT resources and initiatives. Questions remain regarding the agency's ability to enforce the guidance consistently across TSA programs. Program managers are not consistently aware of the existing review boards and have a limited understanding of the decision making process.

Further, we reported that TSA's decentralized IT budget hinders visibility of IT spending across the organization. As the agency evolved in a decentralized manner, the CIO has had no official or substantive role in budgeting or planning for IT programs initiated in other offices apart from the IT Division. As a result, the CIO frequently is not consulted on significant technology decisions and investments. Some high-profile programs, such as Secure Flight, receive direct funding through appropriations or user-generated fees. Because of its mandated funding, the program has not relied on external support from the IT Division. Such mandated funding also hinders enterprise-wide, long-term IT planning, and reduces opportunities to integrate and leverage existing IT initiatives.

We recommended that the Assistant Administrator for TSA strengthen agency IT management by empowering the CIO with agency-wide IT budget and investment review authority to ensure that IT initiatives and decisions support accomplishment of TSA mission objectives. We also recommended that TSA apply adequate staff resources to strengthen the IT Division in addressing IT needs and support agency-wide operations. The Assistant Administrator concurred with our recommendations and has taken steps to improve the CIO's agency-wide IT budget and investment review authority by expressing support for DHS management directive 0007.1, *Information Technology Integration and Management*. However, IT staffing levels continue to be a concern and have not yet been addressed due to budget constraints.

[7] *Information Technology Management Needs to Be Strengthened at the Transportation Security Administration* (OIG-08-07, October 2007).

Federal Emergency Management Agency (FEMA)

DHS components, such as the Federal Emergency Management Agency (FEMA), have taken steps to improve acquisition management. We reported in February 2009 that FEMA had made progress in improving internal controls over its acquisition process, but identified additional safeguards that FEMA needed to take.[8] For example, we recommended that FEMA establish an internal control board and assess the adequacy of its internal controls annually. In addition, we recommended that FEMA comply with the Federal Acquisition Regulation on contract close out, so that unused funds can be spent to address future needs. FEMA agreed with our recommendations and has begun to address some of the weaknesses identified in the report.

We reported as well in February 2009 that FEMA's Office of Acquisition Management had made progress in implementing best practices into the acquisition process.[9] In our report we noted additional practices that FEMA needs to include, such as:

- Developing a strategic plan that links to the agency plan or outcome-based performance measures that tie to the agency's strategic goals;
- Working with program officials to create a more strategic approach to acquisition planning and management;
- Developing an oversight process to determine the efficiency and effectiveness of the acquisition program; and,
- Creating systems to document and share lessons learned throughout the acquisition function

FEMA concurred with our recommendations and has begun to implement these best practices as well.

The FEMA CIO also faces significant challenges in efforts to improve IT management, budgeting, planning, and investment. We reported in September 2005 that the CIO could not ensure that IT investments were well-integrated or aligned with mission needs.[10] We noted that an inadequate long-term IT strategy, coupled with insufficient IT budget control has resulted in IT systems unable to share information. Subsequently, in May 2008, we reported that FEMA's logistics management systems do not provide complete asset visibility, comprehensive asset management, or integrated information during disaster response.[11] Without effective IT support for its logistics activities, FEMA staff will find it difficult to perform disaster response in an effective, timely manner.

---

[8] *Internal Controls in the FEMA Disaster Acquisition Process* (OIG-09-32, February 2009).
[9] *FEMA's Implementation of Best Practices in the Acquisition Process* (OIG-09-31, February 2009).
[10] *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery* (OIG-05-36, September 2005).
[11] *Logistics Information Systems Need to Be Strengthened at the Federal Emergency Management Agency* (OIG-08-60, May 2008)

Until the IT budget data is fully controlled at the component level and consolidated at the department level, the DHS CIO will not attain complete visibility of IT spending across components, hindering the ability to influence technology decisions and investments.

In summary, the DHS CIO has a responsibility to effectively manage IT acquisitions to promote a unified direction and ensure alignment to departmental goals. However, insufficient department OCIO and component-level OCIO staff and fragmented IT budget and management practices have hindered the department's ability to fully integrate new IT management and acquisitions practices. Once fully implemented and supplied with sufficient resources, the IT management and acquisition mechanisms that DHS has put into place may ensure IT investments fulfill mission and IT goals, thus promoting overall efficiency and effectiveness across the department.

Ms. Chairwoman, this concludes my prepared statement. Thank you for this opportunity and I welcome any questions from you or Members of the Subcommittee.