DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Progress Made In Strengthening DHS Information Technology Management, But Challenges Remain

OIG-08-91

September 2008

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

September 4, 2008

Preface

The Department of Homeland Security, Office of Inspector General, was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the strengths and weaknesses of Information Technology management activities as carried out by the department's Office of the Chief Information Officer. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CFO	Chief Financial Officer
CIO	Chief Information Officer
CPIC	Capital Planning and Investment Control
C&A	Certification and Accreditation
DHS	Department of Homeland Security
EAB	Enterprise Architecture Board
E-Gov	Electronic-Government
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
ICE	U.S. Immigration and Customs Enforcement
IRB	Investment Review Board
IT	Information Technology
ITAR	Information Technology Acquisition Review
ITSO	Information Technology Services Office
MD	Management Directive
OCIO	Office of the Chief Information Officer

Table of Contents/Abbreviations

OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
TSA	Transportation Security Agency
USCG	United States Coast Guard
USCIS	U.S. Citizenship and Immigration Services

Figures

Executive Summary

Creating a unified information technology (IT) infrastructure for effective integration and agency-wide management of IT assets and programs remains a challenge for the Department of Homeland Security (DHS) Chief Information Officer (CIO). In our 2004 report, *Improvements Needed to DHS' Information Technology Management Structure* (OIG-04-30), we said that the DHS CIO was not well positioned with sufficient authority or staffing to manage IT assets and programs. We identified actions that DHS could take to improve IT investment oversight.

We conducted a follow-up audit to examine DHS' efforts to improve its IT management structure and operations. The objectives of this audit were to identify the current DHS CIO management structure and changes made to roles, responsibilities, and guidance for managing IT; determine whether current IT management practices and operations are effective to ensure strategic management of IT investments; and to assess progress in addressing our prior recommendations.

DHS budgets more than $5 billion a year for its IT programs. Since its formation in 2003, DHS has faced significant challenges to establish an effective IT management structure to oversee and guide the department's IT resources. However, DHS has taken steps over the past year to strengthen the CIO's role for centralized management of IT. Specifically, the DHS CIO attained greater authority for leading component CIOs toward a unified IT direction. In addition, the DHS CIO has gained oversight of IT acquisitions by establishing new policies and improving IT investment governance functions. As a result, the DHS CIO is better positioned to guide the department's IT resources. However, continued CIO staffing shortages and inconsistent component-level IT budget practices impede progress. Additionally, DHS' IT management capabilities at the component level, such as IT strategic planning, have not been fully implemented. As a result, the DHS CIO remains hindered in his ability to fully integrate IT management practices to ensure IT investments fulfill mission and infrastructure consolidation goals.

DHS must address these challenges to achieve its IT goals. We recommend that the DHS CIO update the CIO office's staffing plan, ensure that components submit comprehensive budgets, and develop and maintain IT strategic plans and enterprise architectures aligned to DHS' mission.

Background

The Homeland Security Act of 2002[1] established a Chief Information Officer (CIO) to govern information technology (IT) across the newly created Department of Homeland Security (DHS). The primary goal of the DHS CIO is to transform the department into a high-performing and integrated organization by providing effective technologies and systems to meet DHS' mission needs.

The 22 component agencies that currently make up DHS rely extensively on IT to perform mission operations, as evidenced by DHS' fiscal year 2008 IT budget of over $5 billion. Given the size and significance of DHS' IT investments, effective management of department-wide IT expenditures is critical.

The DHS CIO reports to the Under Secretary for Management and is supported by the Office of the CIO (OCIO), which comprises the Deputy CIO, a Chief of Staff, and a full time OCIO staff with contractor support. The mission of the DHS OCIO is to collaborate with DHS component-level CIOs to align the IT systems and infrastructure in support of missions and activities across the department. The OCIO is organized into five major offices, as depicted in Figure 1 below.

Office of the Chief Information Officer Organization Chart

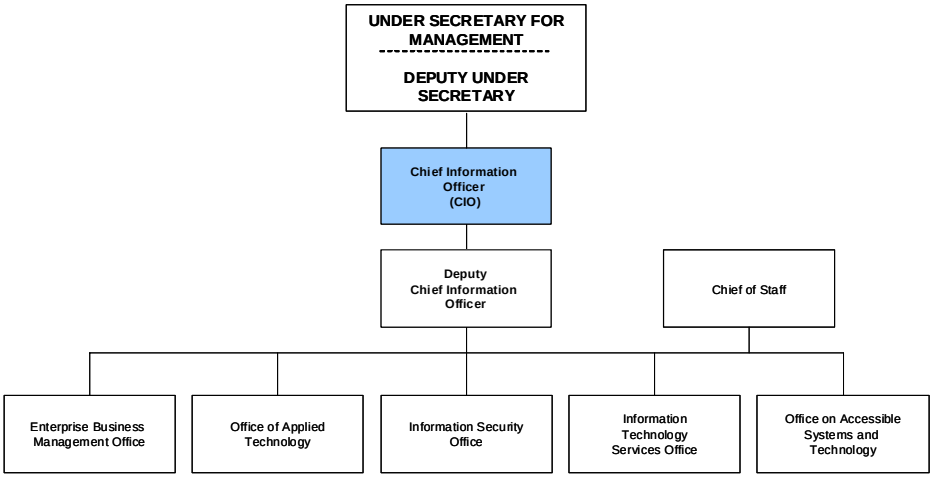


Figure 1: Office of the Chief Information Officer Organization Chart

The Enterprise Business Management Office oversees IT budget functions and manages the department's IT investments to align to mission priorities and planned targets. The Office of Applied Technology has primary

[1] Public Law 107-296, November 25, 2002.

responsibility for the department's enterprise architecture. The Information Security Office provides oversight to ensure a secure and trusted computing environment that enables the department to effectively share information in support of its mission. The Information Technology Services Office is responsible for managing the IT infrastructure including network, email, Internet, telecommunications infrastructure, and end-user services to users in the DHS headquarters offices. The Office of Accessible Systems and Technology leads department-wide implementation of Section 508 of the *Rehabilitation Act of 1973*,[2] providing technical support and training to ensure DHS employees and customers with disabilities have equal access to information and data.

In 2004, we reported challenges in the DHS CIO's ability to effectively manage IT resources and capabilities to fulfill the department's diverse and unique missions.[3] Specifically, we found that the DHS CIO did not have sufficient oversight of IT investments or support to execute central IT direction due to a lack of authority within the DHS leadership structure. Additionally, the CIO did not have sufficient staffing or a defined component-level CIO reporting relationship. Based on these findings, we recommended that DHS:

- Centralize IT support services, provide the CIO with authority to influence department-wide IT investments and strategies;
- Document and communicate the roles of component-level CIOs;
- Provide the DHS OCIO with the necessary staffing resources; and
- Assign the DHS CIO a key role in all levels of the department's investment review process.

Results of Audit

CIO Organizational Structure Improved

DHS has improved the DHS CIO's role in managing IT by better defining CIO responsibilities and reinforcing authority over IT department-wide. In addition, DHS has strengthened the DHS CIO's management structure and reporting relationships to the component-level CIOs. As a result, the DHS CIO is better positioned to meet the department's IT challenges and govern shared IT programs and services as well as to help better direct the components' mission and supporting technologies in a concerted manner.

[2] 29 U.S.C. Section 794d.
[3] *Improvements Needed to DHS' Information Technology Management Structure*, OIG-04-30, July 2004.

DHS IT Management Roles and Responsibilities are Better Defined

Federal regulations provide guidance for establishing an effective management structure to govern IT, which has become increasingly critical to federal agency success. The *Clinger-Cohen Act of 1996*[4] requires that federal departments and agencies establish CIOs to institute, guide, and oversee frameworks for managing IT department-wide. Additionally, the *Homeland Security Act of 2002*[5] sets forth responsibilities to execute IT planning, budgeting, infrastructure management, systems development, IT human capital planning, and support services functions. With these responsibilities, the DHS CIO faces the complex challenge of managing a wide range of IT assets and programs for the third largest department of the federal government.

According to federal guidelines, executive agencies benefit from positioning the CIO as a member of the senior executive team with sufficient accountability and responsibility to manage IT across organizational units. However, in 2004, the DHS CIO was not a member of the senior executive management team and lacked the authority to strategically manage the department's technology assets and programs. In addition, there was no formal reporting relationship between the DHS CIO and the CIOs of major component organizations, which hindered department-wide support for a central IT direction.

In March 2007, DHS issued DHS Management Directive (MD) 0007.1: *Information Technology Integration and Management*. This directive is the principal document for leading, governing, integrating, and managing the IT function throughout DHS. As illustrated in Figure 2, the directive addressed several of the IT management challenges that we raised in 2004.

Prior IT Management Challenges	Management Directive 0007.1 Changes
• DHS CIO lacked authority in leadership structure	• Solidified DHS CIO's reporting relationship with the Under Secretary for Management • Authority establishing department IT priorities, policies, processes, standards, guidelines, and procedures reinforced
• Component CIO reporting relationship undefined	• Oversight of component CIOs defined including recruiting, and conducting performance planning and feedback
• Oversight of IT investments Insufficient	• IT acquisition review authority defined • IT budget review authority defined

Figure 2: DHS Management Directive 0007.1 Changes

[4] *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, Section 5125, February 10, 1996.
[5] *Homeland Security Act of 2002*, Public Law 107-296, November 25, 2002.

Specifically, the directive solidified the reporting relationship of the DHS CIO to department leadership and established the CIO's authority over IT management. It also documented the component CIOs' reporting relationship to the DHS CIO.

DHS CIO's Authority Expanded

The MD 0007.1 established the authority and responsibilities of the DHS CIO. The directive sets forth DHS policy that the DHS OCIO shall serve as the foundational DHS organization through which all departmental IT activities and services will be overseen, defined, and measured. It also clarifies the DHS CIO's role to exercise leadership and authority over IT policy and programs department-wide by giving the DHS CIO authority to, among other things:

- Design the structure, processes, and systems to support both departmental and component missions and goals in collaboration with the CIO Council;
- Establish department IT priorities, policies, processes, standards, guidelines, and procedures;
- Conduct IT program reviews and recommend program improvements or corrective actions, including revocation of delegated authorities and cancellation of IT acquisitions, procurements, and initiatives;
- Implement an IT budget strategy for delivering and maintaining enterprise IT solutions and services in conjunction with the DHS Chief Financial Officer; and
- Establish training, development, and certification guidelines for DHS IT professionals.

The directive has improved the DHS CIO's authority within the existing leadership structure by strengthening the position of the DHS CIO. One senior official said that the DHS CIO has considerable cooperation and assistance from DHS leadership to support the CIO's direction for managing IT department-wide.

DHS CIO and Component CIO Responsibilities Defined

Since our 2004 report, DHS has made demonstrable progress toward strengthening the reporting relationships and responsibilities of the DHS CIO in relation to the component-level CIOs. The MD 0007.1 establishes a "dotted-line" reporting relationship from the component CIOs to the DHS CIO. Figure 3 lists the major roles and responsibilities of the DHS and component CIOs.

Department CIO	Component CIOs
• Define the IT organization including structure, priorities, policies, and standards • Lead component CIOs, including recruiting, performance review, and delegating authorities • Advise and report to senior-level officials on IT • Review of components' IT budgets, acquisitions, and programs • Lead CIO Council and EA Board • Establish the department-level information security program • Establish training guidance	• Deliver IT services to support the component mission • Comply with department policies, processes, standards, and guidelines • Collaborate with DHS CIO to ensure effectiveness of IT programs and resources for enterprise IT solutions • Implement the component-level EA and IT strategic plan • Facilitate communication between component heads and the DHS CIO and CIO Council • Submit IT budget and acquisitions for department CIO review • Participate in CIO Council and EA Board • Develop a component-level information security program

Figure 3: Management Directive 0007.1 CIO Responsibilities

The directive gives the DHS CIO the authority to provide component-level CIOs written performance objectives at the start of the performance cycle, provide input to their rating official on their accomplishments against these objectives, and approve bonus or award recommendations. To solidify department-level oversight, the DHS CIO has the authority to perform an annual assessment of each component's functional performance. The DHS CIO's oversight role is further strengthened with the ability to delegate authorities to component CIOs to ensure appropriate administration of mission services. In addition, component heads must also collaborate with the DHS CIO in recruiting and selecting key IT officials by seeking DHS CIO approval on the qualification standards for positions, candidates identified for consideration, and final selections.

Component CIOs expressed support for the current DHS CIO reporting structure, stating that the degree of oversight is well balanced for IT planning and management. The current reporting relationship to the DHS CIO does not create excessive departmental oversight of component operations. For example, one component CIO stated they are able to effectively carry out their component-level IT leadership responsibilities in parallel to reporting to the DHS CIO.

Increased Oversight of IT Budgets

The MD 0007.1 also provides the DHS CIO with greater authority over component-level IT budgets. Starting in fiscal year 2009, component CIOs must prepare a separate IT budget across all programs and activities within the components. Component heads are to submit these budgets to the DHS CIO for review and approval. Both the DHS OCIO and component-level CIOs support the new budget process. DHS OCIO officials said the increased budget review responsibilities will greatly

improve the DHS CIO's level of leadership and authority over IT programs department-wide. Most component CIOs said that the process will increase their ability to gain oversight of component-level IT spending by providing them the authority needed to gain access to IT budget data throughout their agency. According to the U.S. Citizenship and Immigration Services (USCIS) CIO, the IT budget requirements set forth in the MD 0007.1 are providing greater visibility into actual IT spending that previously might not have been categorized as IT spending. Additionally, a 2007 Office of Inspector General (OIG) report[6] said that the Transportation Security Administration (TSA) had little centralized IT budget authority. However, according to the TSA Deputy CIO, the directive has improved visibility into IT spending.

The DHS OCIO has coordinated with component CIOs to ensure their understanding of the budget review process. For example, the DHS OCIO has conducted program reviews and held informal meetings with components to discuss IT budget data and answer their questions about the process. DHS OCIO officials said that this has been especially helpful for components with large budgets that may have more items for review.

The DHS CIO also provided a briefing of the fiscal years 2010 to 2014 IT budget review process at the January 2008 CIO Council meeting. The briefing was well received by component CIOs, who said that the guidance provided will help align and consolidate IT throughout the department. For example, the budget guidance identified specific enterprise IT targets, such as common data center and network technology, which will drive the department to move to a common infrastructure. These efforts by the DHS OCIO have increased understanding of the budget process in general and, more specifically, of what the components are expected to provide to DHS for their IT budget every year. As a result, components are better able to create component-level budgets that meet department expectations and that can be rolled up to allow for improved planning of department-wide IT spending.

IT Investment Management Improvements

DHS has improved its IT investment management through more effective governance bodies and activities. In addition, the DHS CIO's role in the department's investment review process has increased. As a result, the DHS CIO has greater oversight of department-wide IT investments, increasing his ability to achieve centralized management and awareness of all IT systems and initiatives.

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

IT Governance Initiatives Increase CIO IT Management Capabilities

According to federal guidance and departmental directives, the CIO is required to implement IT governance structures to ensure efficient and effective use of technology resources.[7] The DHS CIO relies on a variety of IT investment governance structures and functions to ensure compliance with IT management policies and promote centralized IT management. Additionally, the DHS OCIO has initiated IT governance improvements to promote centralized IT oversight and increase the DHS CIO's ability to perform IT management functions. Key elements of the DHS IT governance approach involve the CIO Council, an Investment Review Board, the Capital Planning and Investment Control process, an Enterprise Architecture Board, and Portfolio Management process.

DHS CIO Council

The DHS CIO Council was established to set vision and strategy for the IT function and information resources within DHS. Membership is composed of the DHS CIO and Deputy CIO, who chair the council, and all component-level CIOs. The council provides a forum for communication and coordination among its members to achieve departmental IT infrastructure consolidation goals. The council also provides recommendations for the department IT strategic plan and establishes policies, processes, best practices, performance measures, and decision criteria for managing the delivery of IT services. Figure 4 lists the eight major functions of the CIO Council.

DHS CIO Council Functions	
• DHS-wide IT strategic planning • DHS IT governance structures and processes • Information resource management policies, processes, best practices, performance measures, and decision criteria • Advancement of DHS IT priorities	• Opportunities for coordination, consolidation, and information sharing with other agencies • Involvement with high visibility IT projects that have DHS-wide implications • Establishment of appropriate working groups tied to CIO priorities • Communication programs for constituencies

Figure 4: DHS CIO Council Functions

[7] E-*Government Act of 2002*, Public Law No. 107-347, Section 3603 establishes the CIO Council. The *Clinger-Cohen Act of 1996*; OMB Circular A-130, *Management of Federal Information Resources*; and OMB Circular A-11, *Planning, Budgeting, Acquisition and Management of Capital Assets* provide regulations and guidance for investment review and capital planning activities. DHS Management Directive 0007.1, *IT Integration and Management*, establishes the authority and responsibilities of the DHS CIO. DHS Management Directive 1400, *Investment Review Process*, integrates capital planning, budgeting, and acquisition, and management of IT investments to ensure public resources are wisely invested.

In 2004, we reported that the council had evolved into an unstructured information reporting session for CIOs.[8] Lacking a formal structure, meetings were spent providing status updates on IT activities and issues within their organizations rather than focusing on strategic-level collaboration and decision-making. However, the CIO Council has begun to function more effectively as the primary coordination entity between the department-level and component-level CIOs, and has gained a positive reputation as a productive forum for strategic-level collaboration and decision-making since the time of our 2004 report. As a result, the CIO Council has increased the CIOs ability for strategic-level management of IT and collaboration among component stakeholders.

In November 2007, the DHS CIO instituted a secondary, more informal group to improve the effectiveness and efficiency of the CIO Council and promote increased collaboration among component CIOs. This group, referred to as the "Gang of Seven," is composed of CIOs from the seven major components.[9] The group's goal is to build consensus among the largest stakeholders on programs that have potential for DHS-wide impact or on departmental IT policies and standards.

Several component CIOs said that having the opportunity to coordinate within this smaller subset has improved the productivity in larger meetings of the full council. For example, component CIOs used these meetings to coordinate the development of common screening technology for the department and identify concrete steps for the near term. This type of coordination has proven especially critical when new technologies or strategic-level IT direction are being considered.

According to DHS OCIO leadership, the CIO Council has become a more effective mechanism for building consensus among components and providing an advisory board for the DHS CIO. A senior IT official said the council is functioning effectively as a primary means of communication across the component CIOs. As a result of the efforts of the council, several component CIOs said the relationship between component CIOs now is very collaborative, resulting in greatly improved productivity and communications. For example, CIOs have comprehensive discussions on their stewardship roles and the IT infrastructure process.

[8] *Improvements Needed to DHS' Information Technology Management Structure*, OIG-04-30, July 2004.
[9] The seven major operational components of DHS are the Transportation Security Administration (TSA), U.S. Customs and Border Protection (USCBP), U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (USICE), U.S. Secret Service (USSS), the Federal Emergency Management Agency (FEMA), and U.S. Coast Guard (USCG).

Investment Review Board

Currently, the Office of the Chief Procurement Officer and the DHS CIO are collaborating to refine the investment review process and the corresponding DHS Management Directive 1400, *Investment Review Process*. One key aspect of this effort involves the Investment Review Board (IRB), the governance board responsible for providing senior managers with visibility, oversight, and accountability for investments. Although the DHS CIO does not directly oversee IRB activities, he plays a major role in reviewing IT investments that reach the IRB threshold. The revised process incorporates extensive input from the OCIO and will include the CIO in the investment review process. This input should ensure further CIO involvement in IT investment reviews.

Capital Planning and Investment Control

The DHS OCIO is working to enhance the Capital Planning and Investment Control (CPIC) business case submission process. As part of the CPIC process, components are required to submit business plans for IT investments to demonstrate adequate planning. To ensure that IT investments are based on a solid business case, the OCIO established a group to govern the CPIC process throughout the department. Projects are reviewed for approval and progress, primarily based on "Exhibit 300" business case documentation, which is developed for submission to the Office of Management and Budget (OMB) pursuant to the annual budget process.

To aid the CPIC process, CPIC administrators from each component act as liaisons between the department and the component programs. These administrators meet every 2 weeks with the DHS OCIO to review issues and identify process improvements. Additionally, the OCIO offers training for CPIC administrators, including lessons learned that are captured annually. However, one challenge for the OCIO has been that the administrators are sometimes contractors rather than government employees. Because historically there has been high turnover with the contractors, the OCIO must spend extra time retraining and re-educating the new CPIC administrators. Further, contractors sometimes lack access and communication channels to component leadership, limiting the effectiveness of the group for components with contractor representation.

Enterprise Architecture Board

The Enterprise Architecture Board (EAB) is an investment review mechanism that has improved department-wide IT management functions. Consistent with the investment review process, EAB is responsible for

reviewing and making recommendations to the DHS CIO for approving individual investments. Also, the board is responsible for ensuring that each IT investment aligns with the DHS enterprise architecture and is approved before submission to the CIO for final approval and inclusion in the annual budget submission. Finally, the EAB is responsible for directing, overseeing, and approving the DHS enterprise architecture and ensuring compliance with OMB federal enterprise architecture guidance. Membership is composed of the DHS CIO and Deputy CIO, component CIOs, Chief Financial Office designee, Chief Procurement Office designee, business unit and program representatives, information officers, and directorates/organizational elements.

Portfolio Management

To augment investment review processes, the OCIO has recently begun a portfolio management program. The DHS portfolio management approach aims to establish portfolios, based on DHS mission areas, strategic goals, and objectives. Several pilot portfolio initiatives were conducted by the DHS CIO in fiscal year 2007 to prepare for department-wide implementation in fiscal year 2008. At the time of our review, 22 IT portfolios have been established by the DHS CIO, with 6 assigned to Portfolio Managers. One primary goal of the portfolio program is to align IT investments with strategic objectives across all of DHS. As a result, the DHS CIO will increase visibility of IT spending, thereby more effectively managing all IT investments across the department.

Absent this, there has been limited visibility into relationships between IT assets and investments across the department. Going forward, the DHS CIO will designate a portfolio manager for each of the DHS IT portfolios to provide recommendations and perform analysis for investments within their assigned portfolio. The DHS IT portfolio management program will augment existing budget, acquisition, and review processes and decision-forums. Within each portfolio, target architecture and transition plans will be established to ensure that investments within portfolios effectively meet mission goals and objectives.

Once portfolio management is implemented, the DHS CIO will increase line-of-sight visibility across all IT investments and the ability to eliminate spending on duplicative IT assets, to integrate and manage IT investments agency-wide. According to one OCIO senior official, this process has already been successful in giving the DHS CIO visibility into investments and aligning them to mission and goals.

Increased DHS CIO Management Oversight of IT Acquisitions

The *Clinger-Cohen Act of 1996* assigns CIOs responsibility for ensuring effective acquisition of information technology resources.[10] In 2004, the DHS CIO did not have sufficient visibility or approval authority for department-wide IT investments. Based on Management Directive 1400, the DHS CIO's primary IT investment review responsibility was limited to "level-three investments," which had a cost of $1-5 million annually or lifecycle costs of $5-20 million.[11] Therefore, the DHS CIO was not the principal proponent for level-one and level-two investments, which are critical programs with contract costs over $5 million and lifecycle costs over $20 million. Rather, the IRB, headed by the Deputy Secretary, was responsible for reviewing both non-IT and IT investments for levels one and two. With this structure, the DHS CIO had minimal control over high priority IT investments, limiting the ability for centralized management and awareness of all IT systems and initiatives.

The DHS CIO has made progress by establishing an acquisition review process to improve CIO oversight of IT spending. In November 2006, under MD 0007.1, the DHS OCIO implemented a new IT acquisition review (ITAR) process to review and approve all department-wide IT acquisitions exceeding $2.5 million. The ITAR process steps are described in Figure 5.

Component CIOs must submit an acquisition request package to the DHS OCIO for review and approval. An OCIO coordinator reviews the package for completeness and provides it to OCIO subject matter experts for evaluation. The CIO staff makes acquisition decisions on the request package at their twice-weekly meetings. Following the OCIO's review, the Acquisition Review Board either approves the acquisition or sends it back to the components with specific conditions for the component to address. The DHS CIO Acquisition Review Board consists of the DHS CIO direct reports. This body makes the final recommendation on an acquisition request.

[10] *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, Section 5125, February 10, 1996.
[11] Department of Homeland Security, Management Directive 1400, *Investment Review Process*.

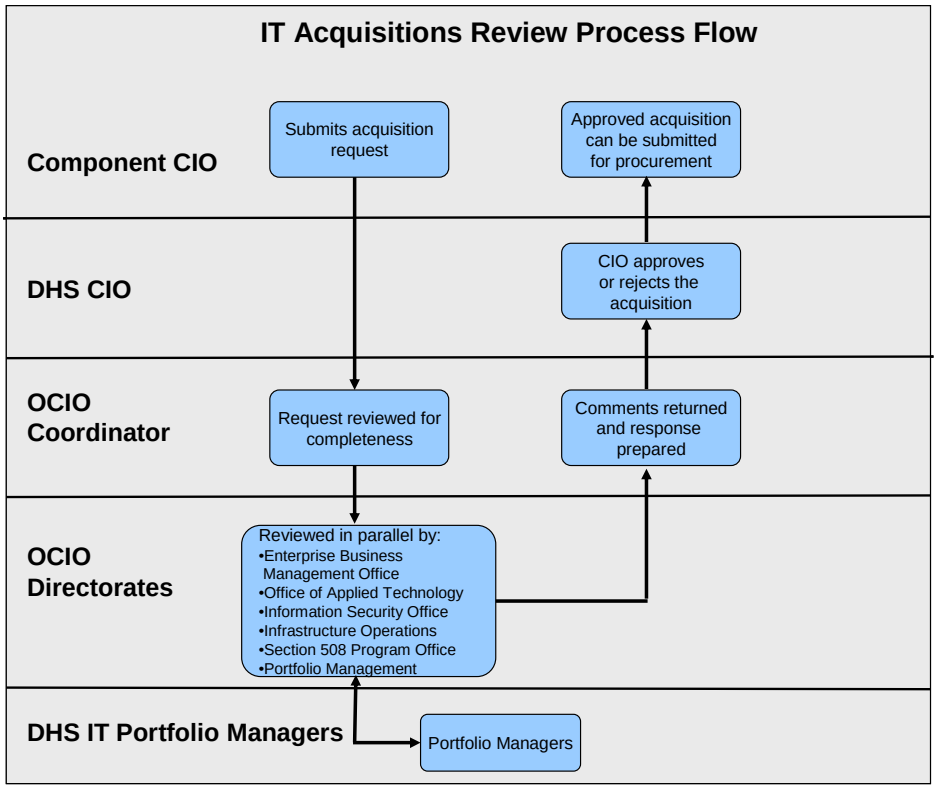


Figure 5: IT Acquisitions Review Process Flow

Many of the larger component-level CIOs have assigned ITAR coordinators to administer their IT acquisition packages. These coordinators track and manage requests throughout the process and attend regular coordinator meetings. According to a DHS OCIO official, components that have implemented the process with assigned coordinators are realizing greater benefits, such as shorter review times and fewer conditions. For example, acquisition requests from coordinators resulted in a review time of 16 days, as opposed to an average of over 30 days for all requests. The TSA ITAR coordinator said that this approach has been helpful, with significant benefits stemming from the quarterly coordinator meetings, which provide opportunities for collaboration with other components to share ideas.

The DHS CIO has taken steps to ensure effective implementation of the ITAR process. For example, to obtain buy-in and participation, the OCIO provided a draft of the MD 0007.1 to the components for review and comment. Component-level CIOs provided feedback on how to improve the process, as well as input on their concerns about the challenges components would face to comply with process requirements. The OCIO incorporated many of the components' comments and suggestions into the final version. In addition, the DHS CIO has also issued an *ITAR Review*

Guide that defines the major steps and responsibilities in the review process.

The DHS CIO continues to communicate the ITAR process to stakeholders to improve its execution. In January 2008, the DHS OCIO held a meeting to educate components on the high-level goals of the ITAR process. DHS OCIO officials also lead ongoing acquisition review coordination meetings to gain additional feedback from components. During these meetings, ITAR coordinators and stakeholders may raise issues and identify process improvements for discussion, many of which are addressed by the OCIO. For example, components must complete a checklist as part of the acquisition package. Several components said that the checklist, which contains 167 questions and requires a great deal of time to complete, is too long. Although the checklist had already been revised and shortened once, the OCIO plans to further update the acquisition review questionnaire to make it easier for components to use.

Impact of Acquisition Review

Although the ITAR process has been operating for only 1 year, there is early evidence that the DHS CIO has had a greater degree of impact on IT decisions department-wide. For example, the OCIO reviewed 243 acquisitions within the ITAR process from November 2006 through September 2007, totaling approximately $3.2 billion. According to budget figures collected by the OCIO, these IT acquisitions reviewed accounted for approximately 57% of the total DHS IT budget of $5.6 billion in fiscal year 2007. In this same fiscal year, the review process identified 132 acquisitions, or 54% of the 243 submitted, that had issues components needed to resolve.

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 networks and data centers. Consolidation of component networks and data centers is an element of the DHS CIO's goal to establish "one infrastructure" for the department to facilitate data sharing, security, and efficiency. Through the review process, the CIO has validated component IT plans to ensure commitment to move component-wide area network segments to a common network, as well as to consolidate assets at the enterprise data centers and transition to DHS' Network Operations Center and Security Operations Center.

Additionally, the ITAR process has promoted enterprise architecture and portfolio alignment by ensuring that IT initiatives adhere to established

targets and goals. The ITAR process has increased compliance with the DHS enterprise architecture, enabling the DHS CIO to direct IT efforts to align to target architecture goals. During the initial year of the ITAR process, the number of programs reviewed by the EAB has increased 50%. Additionally, the DHS OCIO directed components to conform to DHS enterprise architecture standards during the review process. For example, TSA planned to create an E-authentication solution for its Alien Flight School Program. However, during the ITAR process, the OCIO recognized that TSA's 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. A TSA OCIO official said that TSA has experienced benefits from the checkpoint established within its procurement office to ensure that all IT acquisitions below $2.5 million go through the required component-level review. Consequently, the TSA CIO reviewed 113 requests under $2.5 million for a total of $70.1 million during fiscal year 2007.

The TSA CIO has more visibility of IT initiatives and, therefore, the ability to consolidate IT requirements and identify other opportunities to decrease costs. The TSA OCIO already has identified opportunities to use more enterprise licenses for products, such as security software, and consolidate IT support contracts that were disorganized across the agency, resulting in cost savings. TSA officials believe that this process has been valuable and provides needed insight on agency-level IT spending and initiatives.

Challenges Remain for Effective Management of IT

Although the DHS CIO has gained increased authority and oversight to better manage department-wide IT investments, significant challenges remain. Specifically, DHS OCIO staffing levels remain insufficient to effectively carry out new IT management responsibilities. Further, component CIOs lack visibility over IT spending, hindering their ability to meet the department's IT budget reporting requirements. Finally, benefits of the IT acquisitions review process are limited until all department programs and CIOs comply with new requirements defined in MD 0007.1. These challenges must be addressed for the DHS CIO to achieve benefits of centralized management of the department's IT, such as cost savings and infrastructure consolidation.

DHS CIO's Staffing Levels Remain Insufficient

In 2004, the DHS CIO had limited staff resources to assist in carrying out the IT management activities needed to support the department. Although DHS has provided the DHS CIO with additional resources, the OCIO continues to experience significant staffing shortages. This has limited the DHS CIO's ability to effectively execute department-wide IT management functions, such as the ITAR process.

In 2004, we reported that DHS CIO staff resources were inadequate.[12] At that time, the CIO was authorized to hire 65 employees to support over 180,000 employees. However, only 49, or approximately 75%, of those positions were filled. In December 2007, the DHS OCIO was authorized to hire 111 employees across the five offices within the OCIO to support over 208,000 employees. However, only 71, or approximately 64%, of the authorized positions were filled. Figure 6 shows a comparison of the 2004 staffing levels to the levels in 2007.

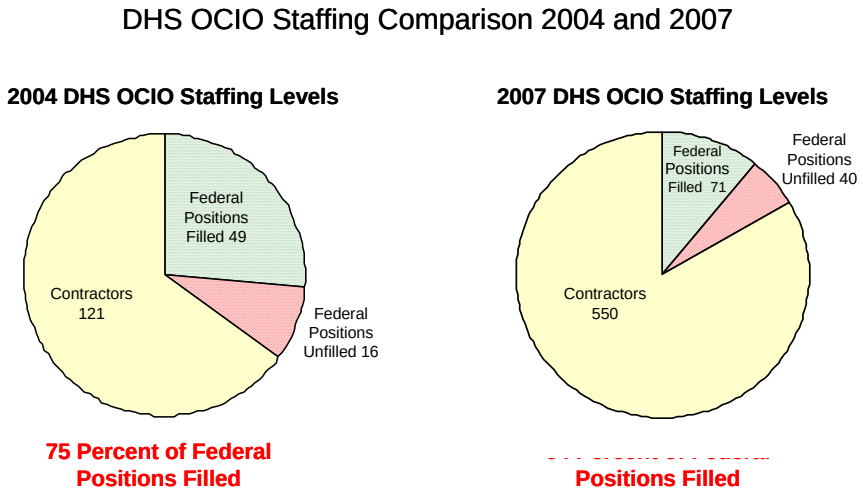


Figure 6: DHS OCIO Staffing Levels: Comparison of 2004 and 2007

The OCIO continues to rely heavily on contractor staff, which accounted for approximately 83% of total staff, to perform OCIO functions. Specifically, contractors assist with initiatives such as E-government (E-Gov), portfolio management, and capital planning. Although the OCIO sees benefits from using contractors to help accomplish such initiatives, there are also disadvantages.

For example, contractors are regularly reassigned or return to their home offices; this means the OCIO has to continuously train new contractors,

[12] *Improvements needed to DHS' Information Technology Management Structure*, OIG-04-30, July 2004.

resulting in less time to work proactively in other areas. The DHS OCIO is encouraging management staff to seek opportunities to convert positions from contractor to full-time government employees. With this approach, the OCIO staffing leadership hopes to increase its federal staff.

OCIO staffing officials said that it has been difficult to hire and retain qualified staff to fill its authorized positions. They attributed hiring difficulties, in part, to the complex and lengthy hiring process within the federal government, which can be burdensome and lengthy. For example, the OCIO must comply with Office of Personnel Management (OPM) standards and guidelines to develop new position descriptions before filling open positions. Further, all OCIO employees must obtain a classified clearance, which often delays hiring efforts. At the time of our review, OPM's Federal Investigative Services Division said it took an average of 65 days to hire a new employee undergoing the background investigation process.

Once positions are filled, there are recurring difficulties with employee retention. The OCIO has experienced turnover rates of approximately 47% each year for the past 2 years. Officials cited the work environment in OCIO as the leading cause for high staff turnover. Specifically, inadequate staffing results in employees working frequent overtime to keep up with the day-to-day demands for IT services and support functions. In this environment, employees get "burned out" from working long hours and they leave. This creates a repetitive cycle of hiring new personnel who must work long hours to meet job demands. As a result, there is little continuity and initiatives often do not get carried over as staff leave. For example, as new management-level staff come in and evaluate ongoing initiatives, efforts are reprioritized and initiatives may be canceled. In this environment, historical context on programs and initiatives is lost.

The OCIO also attributed the high attrition rates to employees moving to private companies or other federal agencies to gain salary or benefits unavailable at the OCIO. The OCIO staffing official who conducts exit interviews said that one primary reason for staff leaving is that they are able to obtain positions that provide the opportunity to work a normal schedule for a commensurate level of pay. The OCIO has developed incentives to provide bonuses and awards to improve retention.

To augment its staff resources, the OCIO has employed a "steward model" to accomplish IT services and meet infrastructure consolidation goals. Under the steward model, components are named as stewards over a domain, such as networks, and hold responsibility for the total performance of the domain project. With this approach, the OCIO is able

to leverage the work being completed at the component level, thereby gaining the IT staff resources and expertise necessary to execute large initiatives.

According to multiple component-level CIOs**,** the steward approach has yielded benefits, such as cost savings, and has enabled the department to make significant progress meeting infrastructure consolidation goals. The steward approach has been most beneficial to the IT Services Office (ITSO), which has the most significant staff shortages within the OCIO. ITSO is responsible for administering department-wide IT support services, such as the infrastructure transformation program. However, at the time of our review, ITSO was staffed at only 60% of its total authorized staffing level. The steward approach has enabled ITSO to meet department-wide IT infrastructure transformation program goals despite inadequate staffing.

Inadequate Staff Resources Limit Effectiveness

The lack of adequate staffing has hindered the DHS CIO's ability to execute the increasing number of department-wide IT management responsibilities. For example, the Enterprise Business Management Office has six federal employees who are tasked to manage multiple enterprise business functions, including E-Gov, CPIC, portfolio management, and the ITAR process. Several component-level CIOs expressed concern with the Enterprise Business Management Office's ability to accomplish these functions with their limited staff.

Specifically, staffing shortages have created significant challenges in meeting the demands to execute the new ITAR process. For example, MD 0007.1 requires the DHS OCIO to provide comments and recommendations on proposed IT acquisitions within 10 business days of receiving the documentation. However, on average, it took 19.6 working days for the OCIO to process IT acquisition requests, with review timing peaking at over 30 days in fiscal year 2007 before additional resources became available. As a result, some components said that the delays affected the time needed to obtain complex acquisitions, making it difficult to keep IT projects on schedule and meet deadlines for implementing high-profile projects.

Inadequate staffing also limits the Enterprise Business Management Office's ability to implement improvements to the ITAR process. For example, plans are in place to upgrade the submissions of acquisitions request packages from the existing email and database to a web-based functionality. Additionally, the ITAR process will be moved to a new automated tracking system to allow components to track the progress of

acquisitions submitted to the OCIO. Both efforts are expected to improve review times and increase collaboration among components and department stakeholders. However, with limited staffing resources in the OCIO, automating the ITAR submission process has not received priority attention resulting in continued use of an inefficient work-around. The Enterprise Business Management office also plans to increase the usage of data collected with component's IT acquisitions packages. For example, the Deputy CIO said that this data could be used to consolidate operations and maintenance acquisition as components move to enterprise data centers. However, it does not have the staff or time to fully analyze all the data captured as part of the ITAR process.

Formal Staffing Plan Needed

To address its staffing shortages, the OCIO has developed an informal staffing resource plan to track and manage vacancies and recruiting efforts. According to the OCIO staffing official, the plan also enables the OCIO to track staffing retention, as well as monitor how the office is progressing toward meeting its target staffing goals of hiring an additional 20 to 22 people over the coming year. However, the DHS CIO lacks a formal long-term recruiting and retention strategy. While the current staffing plan enables the OCIO to maintain a holistic view of staffing levels and vacancies, it does not contain a clearly defined strategy, with specific actions and milestones, to assist the CIO in recruiting and retaining full-time employees.

In September 2007, the Government Accountability Office (GAO) reported that DHS had developed an IT human capital plan.[13] Although the plan was largely consistent with official OPM guidance, some recommended practices were only partially addressed. Missing elements include a clearly defined strategy and plan to facilitate human capital changes and workforce planning. DHS officials responsible for developing the plan said that until the missing elements are fully addressed, it is unlikely that the plan will be effectively and efficiently implemented. This, in turn, will continue to put DHS at risk of not having sufficient people with the right knowledge, skills, and abilities to manage and deliver its mission-critical IT systems.

[13] *Information Technology, DHS' Human Capital Plan is Largely Consistent with Relevant Guidance, but Improvements and Implementation Steps are Still Needed*, GAO-07-425, September 2007.

Department-Wide IT Budget Oversight and Authority Limited

The *Clinger-Cohen Act* requires that CIOs review the IT budget within their agency or department to effectively manage IT systems and initiatives as strategic investments.[14] Further, DHS MD 0007.1 requires component CIOs to effectively manage and administer all component IT resources and assets. Specifically, they must ensure that all IT acquisitions in excess of $2.5 million are approved by the DHS CIO before procurement; report purchases under $2.5 million to the DHS CIO monthly, and prepare a separate IT budget across all component programs and activities.

However, due in part to decentralized IT budget practices, DHS component CIOs face challenges to fully execute the new responsibilities to consolidate and report on agency-wide IT spending. Although IT budget authority has increased for both the DHS and component-level CIOs, execution of that authority is hindered within components by fragmented IT budget policies and procedures. In fact, the majority of component CIOs interviewed said that they are constrained by existing IT budget practices, which present challenges to maintain sufficient agency-wide IT budget oversight. As a result, they are not fully engaged in IT budget planning activities for all levels of IT spending. While component CIOs lack the ability to efficiently and effectively report on IT spending, the DHS CIO has limited oversight of IT department-wide.

Figure 7, below, depicts the varying levels of budget authority within the seven major operational components.

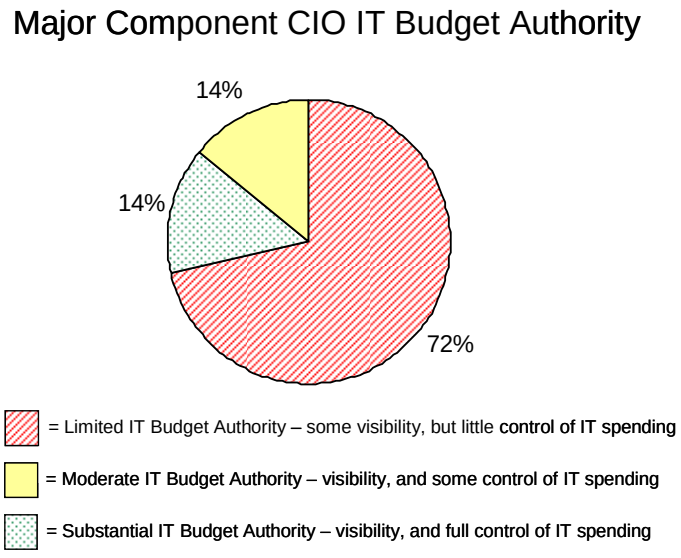


Figure 7: Major Component CIO IT Budget Authority

[14] *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, Section 5125, February 10, 1996.

A number of component CIOs are not fully engaged in program-level IT budget and planning activities. 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 IT budgets that are independent of the CIO. For example, we reported in October 2007 that TSA's CIO had no official or substantive role in IT budgeting or planning outside the IT Division.[15] In this case, the CIO had IT budget authority for only 26% of the total IT spending across the agency, with the remaining IT being managed by programs and offices outside the CIO's authority. As a result, the CIO had limited visibility of systems development activities or implementation plans.

Additionally, a number of component CIOs said challenges stem from complex budget tracking and inconsistent accounting practices, such as uniform standards for categorizing IT spending across the agency. According to several CIOs, IT spending is often improperly categorized, making it difficult to compile an agency-wide IT budget. For example, FEMA OCIO officials said that it is a complex process to separate out IT spending from the overall project because the IT is often rolled into the overall project costs.

Component CIOs are making efforts to centralize component-wide IT spending to better meet the requirements for reporting IT budget data to the department CIO. However, component CIOs said it requires a significant effort to centralize existing fragmented IT budget practices. For example, the Coast Guard is attempting to centralize its IT budgeting functions, but expects it to be a long-term effort. The Coast Guard CIO is developing a process to review component IT spending under $2.5 million. Since it is not cost-effective to look at all purchases, the CIO is determining what the minimum dollar threshold should be. The CIO expects this process also will increase his ability to review common IT purchases, such as radios, to ensure interoperability.

As a result, component CIOs may not be able to accomplish department IT budget responsibilities or reporting requirements until existing component-level budget functions are centralized and updated. Although component CIOs are not required to provide an IT budget to the DHS CIO until fiscal year 2009, some components attempted to meet an initial FY 2008 reporting deadline in April, 2007. Senior DHS CIO officials confirmed that it was a challenge for several component CIOs to provide budget information to the DHS CIO for the initial reporting deadline due

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

to the short timeframe for consolidating IT budgets. DHS OCIO officials said that some components were better able gather the data and create a component IT budget than others.

Until IT budget data is fully 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. This also limits the ability to remediate IT budget issues prior to submission to OMB.

Improvements Needed for IT Acquisition Reviews

The ITAR process has not yet achieved full impact on department-wide IT spending since its implementation in November 2006 due to limited compliance by DHS programs and components. Specifically, in fiscal year 2007, only 57% of the department's estimated $5.6 billion IT budget was evaluated through the ITAR process. According to the DHS OCIO, this is due in part to incomplete agency compliance, as well as the level of effort to implement and administer the acquisition process at the department and component levels.

Additionally, not all department-wide programs have embraced the new process. DHS OCIO officials said that this is more apparent with programs that have direct congressional funding or high profile visibility such as Custom and Border Protection's Secure Border Initiative (SBI-Net). Consequently, these programs are often managed outside of the ITAR process by executive leadership boards that include the DHS Deputy Secretary. As a result, department-wide IT acquisitions oversight remains limited while significant portions of IT acquisitions are not yet being reviewed to ensure alignment with IT policy, standards, objectives, and goals.

Further challenges in implementing the ITAR process stem from the level of effort for component CIOs to incorporate the new ITAR process without any additional staff or budget resources. In most cases, this is a new process not currently performed as part of existing IT acquisitions at the component level. Most component CIOs said that the ITAR process has increased the administrative burden of the component CIOs without adding additional budget or staff resources to assist. Specifically, CIOs said that preparing IT acquisition requests to submit to the DHS CIO requires a significant amount of time and effort, which has increased their workload. However, most components reported they lacked sufficient staff to successfully implement the processes. Component CIOs are putting staff in place and establishing new policies and procedures to more effectively execute the new IT acquisitions process.

Likewise, several components have plans to update their existing IT acquisitions workflow in order to begin conducting reviews for acquisitions under $2.5 million. For example, TSA is establishing a review team of eight subject matter experts to review IT acquisition requests under $2.5 million. However, there is a challenge to obtain staffing with sufficient time or experience to begin the new duties immediately and with minimal training. A separate component, the United States Coast Guard (USCG), is creating a new acquisition office to augment the CIOs ability to administer IT acquisition reviews. In addition to performing the required ITAR functions, the office will serve as a liaison to funnel relevant information between the department and subject matter experts.

DHS IT Management Scorecard Ratings

To determine whether current DHS-level IT management practices and operations are effective, we conducted a high-level assessment of DHS' current IT management capabilities. The purpose of this scorecard is to demonstrate where DHS has strengthened its IT management. The scorecard includes DHS CIO functions as well as the same functions within the seven largest DHS component-level CIO offices. A measurement of components' capabilities is included to provide a more complete perspective on department-wide capabilities.

The focus of this assessment was to identify progress made implementing the following six IT management capability areas:

- IT Budget Oversight: Ensures visibility into IT spending and alignment to the IT strategic direction.
- IT Strategic Planning: Provides a strategy to align the IT organization to support mission and business priorities.
- Enterprise Architecture: Functions as a blueprint to guide IT investments for the organization.
- Portfolio Management: Improves leadership's ability to understand important interrelationships between IT investments and department priorities and goals.
- Capital Planning and Investment Control: Improves the allocation of resources in order to benefit the strategic needs of the department.
- IT Security: Ensures protection that is commensurate with the harm that would result from unauthorized access to information.

These six elements were selected based on IT management capabilities required by federal and DHS guidelines to enable CIOs to manage IT department-wide. The ratings applied to each capability were based on a

four-tiered scale ranging from "Little" progress to "Substantial" progress. Each capability was rated based on the extent to which the capability has been planned and/or implemented, as well as the extent to which the capability is able to provide IT management benefits to the organization. Figure 8 below lists the levels and definitions for our ratings.

Progress Level	Definition
Little	Plans are in place for this capability, but the capability has not been fully implemented
Some	The capability is partially implemented, with limited IT management benefits realized
Moderate	The capability is implemented with moderate IT management benefits realized
Substantial	The capability is implemented with substantial IT management benefits realized

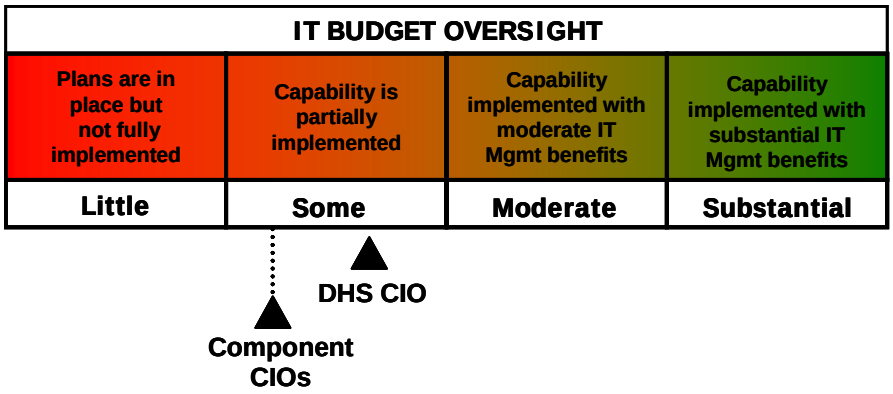
Figure 8: Progress Levels for OIG Scorecard Elements

IT Budget Oversight

The DHS CIO has demonstrated "some" progress in increasing department-wide visibility of the IT budget across DHS. As a result of increased department-wide IT spending visibility, the DHS CIO has also made improvements conducting department-wide IT budget functions. The *Clinger-Cohen Act* requires federal CIOs to ensure that IT is acquired and managed in accordance with agency mission and policies.[16] Coupled with new responsibilities defined in the DHS MD 0007.1, the DHS CIO plans to conduct reviews across the department of all IT and non-IT investments that contain any IT assets and services. The goals for IT budget reviews are to resolve IT budget issues prior to OMB submission, to align IT investments to targets and priorities, and to eliminate redundancies.

Progress in this area was further evidenced by the DHS CIO's fiscal year 2010 IT budget planning guidance, issued in January 2008. According to the DHS OCIO, this guidance will better integrate component IT resource reviews with DHS program and budget reviews. With support of DHS leadership, the DHS OCIO will continue to focus on improving IT budget capabilities.

[16] *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, Section 5125, February 10, 1996.

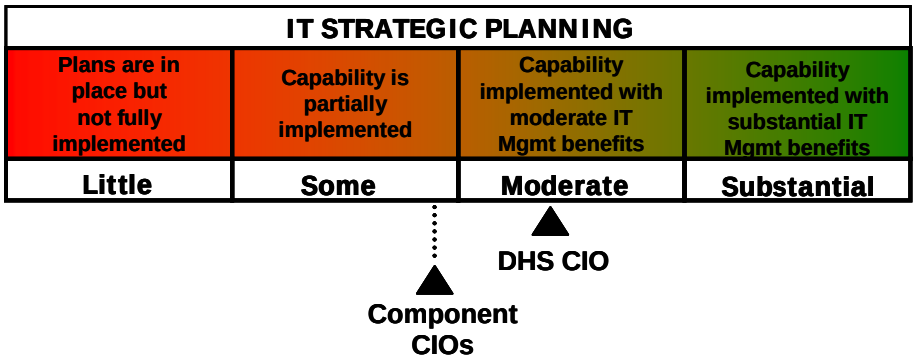


Overall, components demonstrated "some" progress made in conducting IT budget planning and programming functions. Although component-level IT budget responsibilities have increased through the MD 0007.1, over 70% of DHS component CIOs remain hindered by ineffective, decentralized IT budget practices. Most component CIOs plan to further centralize existing IT budget functions in order to meet requirements in the management directive to prepare a component IT budget. For example, many DHS components are implementing initiatives to increase centralized management of IT investments by restructuring and consolidating IT spending accounts that are currently managed by separate offices throughout the agency.

IT Strategic Planning

The DHS CIO's progress in performing IT strategic planning functions is considered "moderate." OMB Circular A-130 instructs agency CIOs to create strategic plans that demonstrate how information resources will be used to improve the productivity, efficiency and effectiveness of government programs.[17] An effective IT strategic plan establishes an approach to align resources and provides a basis for articulating how the IT organization will develop and deliver capabilities to support mission and business priorities. The DHS OCIO has made progress in conducting IT strategic planning by increasing focus on alignment of IT to department goals. Although the current IT planning approach does not fully link technology to mission requirements, the OCIO plans to achieve strategic outcomes and stronger IT alignment to the Secretary's goals. The OCIO is currently updating DHS' IT strategic plan and has communicated the goals within the plan to the CIO Council.

[17] Revision of Office of Management and Budget Circular A-130, Transmittal 4, *Management of Federal Information Resources*, July 1994.



Overall, components made "some" progress in conducting IT strategic planning functions. The MD 0007.1 requires component CIOs to implement a detailed IT strategic plan specific to the component's mission and in support of DHS' mission. As of January 2008, approximately 70% of the component-level CIOs had developed an IT strategic plan. However, there was a wide degree of variance in component-level IT planning capabilities. For example, not all components are consistently able to link strategic goals and objectives with IT investments. Further, although some component CIOs said that they had developed an IT strategic plan, not all are up-to-date or aligned to the DHS mission.

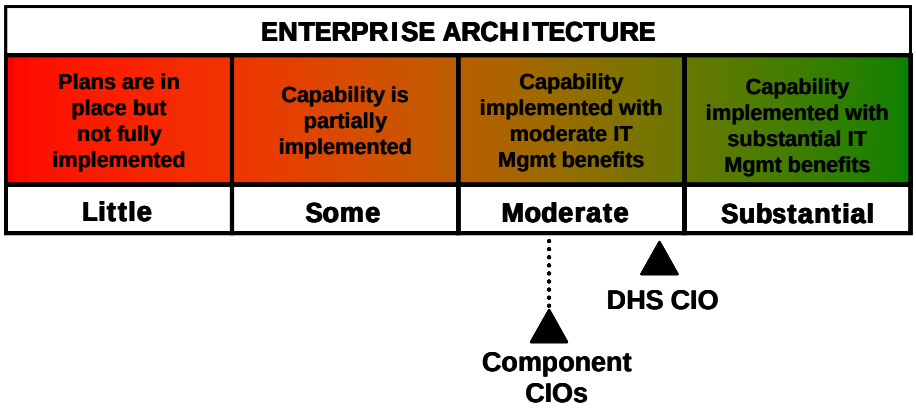
As a result, components may invest in technology that is not effectively aligned with department and agency mission, goals, and business processes. Improvements are planned by some component CIOs who are updating their IT strategic plans. However, until components improve their strategic planning approach, the agency may fall short of its potential to improve business processes and systems.

Enterprise Architecture

The DHS CIO has made "moderate" progress in implementing department-wide enterprise architecture. *The Clinger-Cohen Act* requires that CIOs develop and implement an integrated IT architecture for the agency.[18] An IT architecture functions as a blueprint for the organization to define an operational and technical framework to guide IT investments. Without an effective architecture, there is increased risk that systems will be duplicative, not well integrated, and limited in terms of optimizing mission performance. The DHS-level enterprise architecture has advanced greatly as an effective tool used for reviews and IT management decision-making. Overall, the DHS OCIO has increased its ability to enforce architecture alignment through MD 0007.1. Significant progress is due in part to the ITAR process, which has helped to promote and enforce architecture alignment of component IT investments to the business and technical architectures. Going forward, the OCIO plans to

[18] *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, Section 5125, February 10, 1996.

mature and optimize the department's architecture through performance-based outcomes and to further develop the data architecture in mission-critical areas.



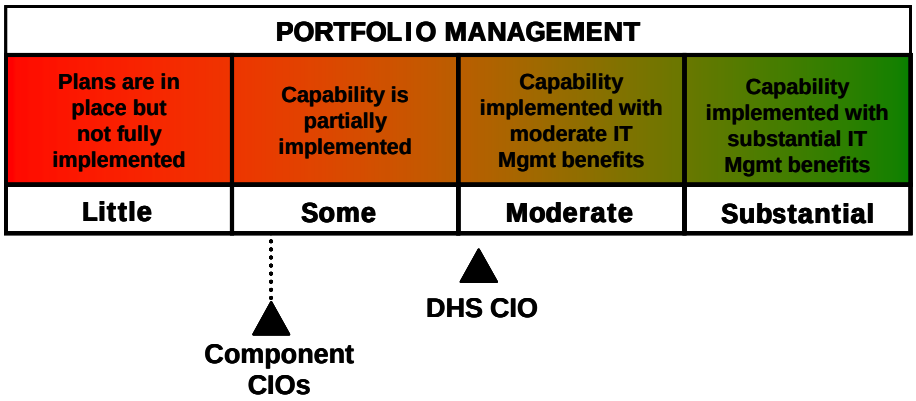
Overall, components received a rating of "moderate" for implementing component-level architectures that align IT investments to the DHS architecture. The MD 0007.1 requires component CIOs to implement a detailed enterprise architecture specific to the component's mission and in support of DHS' mission. As of January 2008, over 70% of the component-level CIOs were able to align IT investments to the department's architecture. Additionally, most components have an architecture defined at the component level that is used for some degree of IT investment decision-making. However, architecture products, such as reference models, definitions of current and future state architectures, and transition plans are in varying stages of development or use by components. Further, a number of components said that their architecture products were out of date or needed to be better defined. For example, one component CIO said that although they have an enterprise architecture in place, it is not fully kept up to date or used.

Portfolio Management

The DHS OCIO has made "moderate" progress in establishing the department's portfolio management capabilities. OMB Circular A-130 instructs agencies to implement a portfolio approach for investments to maximize return for the agency as a whole.[19] The DHS portfolio management program aims to group related IT investments into defined capability areas needed to support strategic goals and missions. Portfolio management improves leadership's visibility into relationships between IT assets and department mission and goals across organizational boundaries.

[19] Revision of Office of Management and Budget Circular A-130, Transmittal 4, *Management of Federal Information Resources*, July 1994.

The DHS OCIO has a solid plan in place to implement portfolio management capabilities in fiscal year 2008. The OCIO has recently finalized plans, along with the first round of documentation and guidance, for a department-level portfolio management approach. Currently, there are 22 defined portfolio areas, six of which are considered priority areas: infrastructure, geospatial, case management, human resources, screening and credentialing, and finance are implemented. Additionally, OCIO has created a portfolio management integrated project team to develop transition plans, measure performance, and standardize the portfolio management process. Although progress is being made, the department is not yet realizing management benefits from the portfolio management program. As a result, the department may miss opportunities for system integration and cost savings.

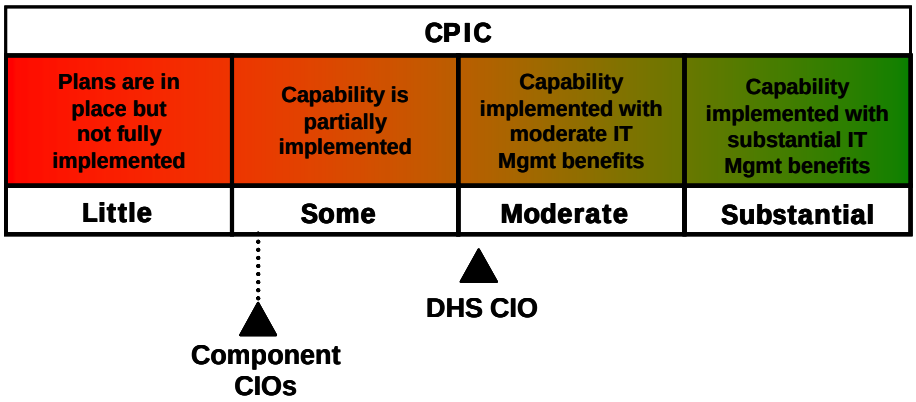


Overall, DHS components have made "some" progress establishing portfolio management capabilities; however, full implementation of this capability widely remains a work in progress. The majority of DHS component-level CIOs have developed a mapping approach to align component IT systems to current DHS-level portfolios. However, as of January 2008, less than half of the seven major component CIOs had implemented a formal portfolio management process at the component level. This is due in part to challenges relating to creating and aligning component specific portfolios to DHS' 22 portfolios.

Many CIOs said that it is a complicated process to fully align their unique mission and business processes to DHS-level IT portfolios. However, Coast Guard officials said that they are working to align all of their IT systems to the DHS portfolios. Through the IT budget review, Coast Guard and DHS OCIO officials identified which portfolios will be associated with each of the systems they have identified in that review. Until this capability is fully implemented, DHS components may continue to invest in systems within organizational silos, and opportunities for consolidation and cost savings may not be realized.

Capital Planning and Investment Control (CPIC)

The DHS OCIO has made "moderate" progress establishing Capital Planning and Investment Control (CPIC) capabilities. The *Clinger-Cohen Act*[20] requires that agencies and departments create a CPIC process to manage the risk and maximize the value of IT acquisitions. The CPIC process is intended to improve the allocation of resources, in compliance with laws and regulations, in order 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 that demonstrate adequate planning. In fiscal year 2007, the 94 DHS programs on the management watch list were reduced to 18. In fiscal year 2008, there are 53 programs, and officials in the OCIO have undertaken efforts to remove these from the list by working with the program managers through the CPIC Administrator's twice-monthly meetings.

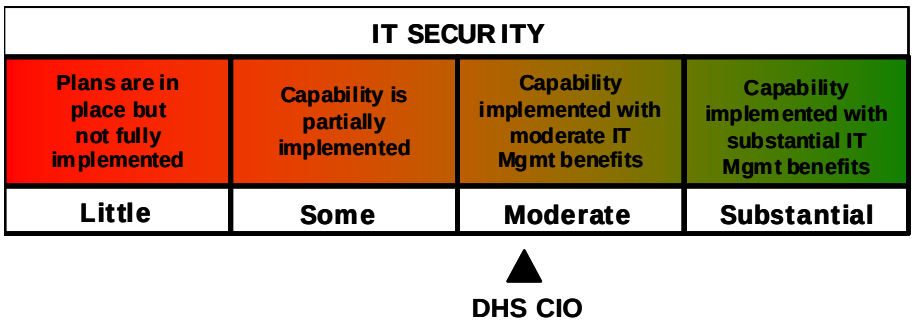


Overall, components demonstrated "some" progress in establishing capital planning capabilities. Most components had not yet achieved an integrated planning and investment management capability. Over 70% of the major DHS components had limited capital planning processes, outside the existing OMB 300 process. However, some component CIOs said that they are creating a CPIC process to integrate with existing governance structures such as the IRB. For example, the ICE IRB resembles a CPIC group with the major disciplines such as security, budget, and Enterprise Architecture all integrated into this process. The ICE CIO said that this process has improved the component's investment review and helps to leverage resources effectively. Overall, there have been improvements in the CPIC process by the components but this process is still being refined.

[20] *Clinger-Cohen Act of 1996*, Public Law 104-106, Division E, Section 5122, February 10, 1996.

IT Security

DHS IT security is rated at "moderate," for progress made over the past two years in compliance with the Federal Information Security Management Act (FISMA). OMB Circular A-130 requires agencies to provide information and systems with protection that is commensurate with the risk and magnitude of the harm that would result from unauthorized access to these assets or their loss, misuse**,** or modification. The CIO has taken an active role in ensuring that components comply with FISMA. In 2007, the CIO requested components to focus on improving areas such as Certification and Accreditation (C&A), annual self-assessments, and plan of action and milestones management. According to the DHS OCIO, additional quality control measures have been implemented to better manage the C&A process. The DHS OCIO also plans to focus on improving disaster recovery and continuity of operations over the coming year.



(Components were not rated on IT security)

Recommendations

We recommend that the DHS CIO:

Recommendation #1: Augment the DHS OCIO Staffing Plan to include specific actions and milestones for recruiting and retaining fulltime employees.

Recommendation #2: Ensure that component CIOs submit comprehensive, standardized IT budgets to the DHS CIO in accordance with Management Directive 0007.1.

Recommendation #3: Ensure that component-level CIOs develop and maintain IT strategic plans and enterprise architectures that align to DHS.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Under Secretary for Management. We have included a copy of the comments in their entirety in Appendix B.

The Under Secretary for Management concurred with our recommendations and provided comments on specific areas within the report. Additionally, the Under Secretary for Management provided an overview on steps being taken to address specific findings and recommendations in the report. We have reviewed management's comments and provide an evaluation of the issues outlined in the comments below.

In response to recommendation 1, the Under Secretary for Management agreed that the Office of the CIO's staffing levels remain insufficient. Accordingly, steps have been taken to accelerate hiring to fill vacant positions. For example, Management Directorate offices are in the process of evaluating whether contractor positions may be converted to create permanent federal positions. Additionally, the CIO Enterprise Business Management Office is developing a staffing management plan that will include individual development plans, training, clearly defined career paths, and performance goals. Management expects this approach to improve the CIO's ability to attract and retain talented government professionals, as well as improving the timeliness of IT acquisitions reviews.

The Under Secretary for Management also agreed that staff resource shortages within the Office of the CIO limit effectiveness in performing information technology acquisitions review. To address this finding, the CIO has distributed ITAR guidance to components and is developing automated capability to improve the process. Such steps are expected to assist the office in meeting the ten-business-day deadline for granting IT acquisition review decisions.

In response to recommendation 2, the Under Secretary for Management stated that the CIO is working closely with the Chief Financial Officer (CFO) and CIO Council to update and communicate budget policies and procedures to components. Specifically, the CIO is working with the CFO to closely integrate IT budget policies and procedures to assess annual component funding requests and ensure their alignment with the department's strategic goals and objectives. Additionally, the CIO Office's Portfolio Management process has been integrated in the IT

budget review process ensuring that the Portfolio Managers have input into the budget recommendations. Through the budget process, continued coordination through the CIO Council will improve consistency in budget data requested by the CIO and the budget data received through the annual resource allocation plan process.

The Under Secretary for Management did not provide a specific response to recommendation 3, relating to component-level CIOs' IT strategic plans and enterprise architecture efforts.

As part of our ongoing responsibility to assess the efficiency, effectiveness, and economy of departmental programs and operations, we conducted a follow-up review of DHS' efforts to improve its IT management structure and operations. The objectives of this review were:

- To identify the current DHS CIO management structure and changes made to establish roles, responsibilities, and guidance for managing IT department-wide;
- To determine whether current DHS-level IT management practices and operations are effective to ensure strategic management of IT investments; and
- To assess progress made in addressing our prior recommendations.

To establish criteria for this audit, we researched and reviewed federal laws and executive guidance related to IT management and CIO governance. We conducted research to obtain testimony, published reports, documents, and news articles regarding the DHS CIO operations and IT management throughout the department. We reviewed pertinent GAO and Office of Inspector General reports to identify prior findings and recommendations. A list of these reports is provided in Appendix C for reference. Using this information, we designed a data collection approach that consisted of focused interviews and documentation analysis to accomplish our audit objectives. We then developed a series of questions and discussion topics to facilitate our interviews.

We interviewed DHS CIO officials and staff to understand the department's strategy and processes for managing IT. Officials within the DHS OCIO described the current IT management environment and how it is evolving. We interviewed senior leadership to understand the division of roles and responsibilities related to developing and implementing department-wide IT management. Additionally, we met with the heads of operations within the Enterprise Business Management Office to discuss the implementation of DHS MD 0007.1 and related processes including newly implemented acquisition and budget review processes. Finally, we met with the heads of the major OCIO offices to obtain feedback on their roles and input to department-wide IT governance processes.

To assess the effectiveness of current IT management practices, we conducted interviews with CIOs from the seven major operational components within DHS: TSA, Customs and Border Patrol (CBP), USCIS, ICE, United States Secret Service (USSS), Federal Emergency Management Agency (FEMA), and USCG. The CIOs from these components provided feedback on their individual IT management environments, reporting relationships, and experiences with IT governance bodies and processes. We also surveyed these CIOs on their current IT

management practices related to strategic planning, enterprise architecture, budget authority, portfolio management, and capital investment processes. We assessed responses and supporting documentation and created an aggregate rating of the current status for components in each of these IT management practices.

The data represented in the scorecard reflects the results of our audit fieldwork and documentation analysis conducted in November 2007 through March 2008. We collected and analyzed data from a variety of sources to determine the scorecard assessment for each of the IT management capabilities discussed in this section. Specifically, the audit team reviewed prior reports and assessments conducted by GAO, and the OIG. Additionally, the audit team requested, reviewed, and analyzed documentation related to the status of each capability from each of the seven components and the department. To obtain department and component CIO input for our assessment, we conducted a verbal survey during interviews.

We conducted this performance audit between November 2007 and February 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions, based on our audit objectives.

The principal OIG points of contact for this audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, and Richard Harsche, Director of Information Management. Major OIG contributors to the audit are identified in Appendix C.

Office of the Under Secretary for Management
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

JUN 11 2008

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General, Information Technology

FROM: Elaine C. Duke
Acting Under Secretary of Management

SUBJECT: Management Directorate Response to OIG Draft Report - *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain*

Management has reviewed the draft report and concurs with the recommendations; however, there is an error on page 16, under unfilled federal positions in 2007, the number should be 40.

Concerning the recommendations and findings of the audit team, Management would like to address the steps being taken to rectify these issues.

Department of Homeland Security Office of the Chief Information Officer's Staffing Levels Remain Insufficient:

We are currently accelerating our hiring to fill the vacant positions. In addition, all of the Management Directorate offices are in the process of evaluating if contractor positions can be converted to permanent Federal positions.

Inadequate Staff Resources Limit Effectiveness (Where there are shortfalls for Information Technology Acquisition Review):

We agree that inadequate staff resources limit effectiveness; however, we have taken steps to reduce this problem. The Chief Information Officer (CIO) has recently distributed Information Technology Acquisition Review (ITAR) Guidance and an ITAR Quick Reference Guide to all components to improve upon the usability of the process. Additionally, the CIO is developing an automated capability for the IT Acquisition Review Process, which will streamline the ITAR process. It is expected that this capability will improve the ability to meet the ten business day deadline for an IT Acquisition Review Decision. This automated capability is expected to be rolled out in the first quarter of Fiscal Year 2009.

Formal Staffing Plan Needed:

The CIO Enterprise Business Management Officer is developing a staffing management plan which will include individual development plans, training, clearly defined career paths, and performance goals. This approach is expected to improve the CIO's ability to attract and retain talented government professionals.

Department-wide IT budget Oversight:

The CIO is working with Chief Financial Officer to closely integrate IT budget policies and procedures to assess annual component funding requests and ensure their alignment with the Department's Strategic Goals and Objectives. Additionally, the CIO Office's Portfolio Management process has been integrated in the IT Budget Review process ensuring that the Portfolio Managers have input into the budget recommendations. Through the budget process, continued coordination through the CIO Council will improve consistency in budget data requested by the CIO and the budget data received through the annual Resource Allocation Plan process.

Improvements Needed for IT Acquisition Review

As mentioned in my response to the "Formal Staffing Plan Needed" concern above, the CIO Enterprise Business Management Officer is developing a staffing management plan which will include individual development plans, training, clearly defined career paths, and performance goals. This approach is expected to improve the CIO's ability to attract and retain talented government professionals.

Should you have any questions, please feel free to contact the Department's Chief Information Officer, Mr. Richard F. Mangogna, at (202) 447-3736.

Appendix C
Related Reports on DHS IT Management

DHS OIG Reports

Improvements Needed to DHS' Information Technology Management Structure, OIG-04-30, July 2004. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_CIOReport_0704.pdf

USCIS Faces Challenges in Modernizing Information Technology, OIG-05-41, September 2005. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_05-41_Sep05.pdf

Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery, OIG-05-36, September 2005. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_05-36_Sep05.pdf

Challenges in FEMA's Flood Map Modernization Program, OIG-05-44, September 2005. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_05-44_Sep05.pdf

US Citizenship and Immigration Services' Progress in Modernizing Information Technology, OIG-07-11, November 2006. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-11_Nov06.pdf

Letter Report: FEMA's Progress in Addressing Information Technology Management Weaknesses, OIG-07-17, December 2006. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-17_Dec06.pdf

Information Technology Management Needs to Be Strengthened at the Transportation Security Administration, OIG-08-07, October 2007. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_08-07_Oct07.pdf

GAO Reports and Testimonies

DEPARTMENT OF HOMELAND SECURITY Formidable Information and Technology Management Challenge Requires Institutional Approach, GAO-04-702, August 2004. http://www.gao.gov/new.items/d04702.pdf

HOMELAND SECURITY Progress Continues, But Challenges Remain on Department's Management of Information Technology, GAO-06-598T, March 2006. http://www.gao.gov/new.items/d06598t.pdf

Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments, GAO-07-424, April 2007. http://www.gao.gov/new.items/d07424.pdf

HOMELAND SECURITY DHS Enterprise Architecture Continues to Evolve But Improvements Needed, GAO-07-564, May 2007. http://www.gao.gov/new.items/d07564.pdf

DHS: Progress Report on Implementation of Mission and Management Functions, GAO-07-454, August 2007.
http://www.gao.gov/new.items/d07454.pdf

Information Technology, DHS' Human Capital Plan is Largely Consistent with Relevant Guidance, but Improvements and Implementation Steps are Still Needed, GAO-07-425, September 2007.
http://www.gao.gov/new.items/d07425.pdf

Information Management Division
Richard Harsche, Director
Kristen Evans, Audit Manager
Steve Staats, Auditor
Shannon Frenyea, Auditor
Beverly Dale, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
Assistant Secretary for Policy
General Counsel
Executive Secretariat
Chief Information Officer
Deputy Chief Information Officer
Chief Financial Officer
Chief Procurement Officer
Director, GAO/OIG Liaison Office
Under Secretary for Management
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- **Call our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at DHSOIGHOTLINE@dhs.gov; or**
- **Write to us at:**

DHS Office of Inspector General/MAIL STOP 2600
Attention: Office of Investigations - Hotline
245 Murray Drive, SW, Building 410
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.