Department of Homeland Security

Office of Inspector General

DHS Information Technology Management Has Improved, But Challenges Remain

OIG-12-82

May 2012

Office of Inspector General

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

Homeland Security

May 4, 2012

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) 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 is to assess progress made in the Department's Office of the Chief Information Officer in implementing an effective information technology management program. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendation herein has been developed to the best knowledge available to our office, and has been discussed in draft with those responsible for implementation. We trust 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.

Frank Deffer
Assistant Inspector General
Information Technology Audits

Table of Contents/Abbreviations

Appendices

Abbreviations

CBP	U.S. Customs and Border Protection
CFO	Chief Financial Officer
CIO	Chief Information Officer
CPIC	Capital Planning and Investment Control
DHS	Department of Homeland Security
DOE	Department of Energy
DOJ	Department of Justice
EBMO	Enterprise Business Management Office
FEMA	Federal Emergency Management Agency
FY	fiscal year
GAO	Government Accountability Office
HHS	Department of Health and Human Services
ICE	Immigration and Customs Enforcement
IT	information technology
MD	management directive

OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
RAP	Resource Allocation Plan
TSA	Transportation Security Administration
USDA	United States Department of Agriculture
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service
VA	Department of Veterans Affairs

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

Creating a unified information technology infrastructure for effective integration and agency-wide management of information technology assets and programs has been a challenge for the Department of Homeland Security (DHS) Chief Information Officer. In 2004 and 2008, we reported that the Chief Information Officer did not have sufficient budget authority or staffing to effectively manage information technology.

We conducted a follow-up audit to determine the Department's progress in implementing an effective information technology management program. The objective of this audit was to assess progress made in establishing Chief Information Officer oversight and authority, achieving integration, improving information technology management functions, and addressing our prior recommendations. Appendix A describes the audit's scope and methodology.

Since 2008, the Chief Information Officer has increased oversight and authority of information technology by reviewing DHS component programs and acquisitions. This has enabled the Chief Information Officer to make strategic recommendations to reduce costs and duplication. The Department has achieved some infrastructure integration goals through data center and network consolidation. Ultimately, the Department expects cost savings through improved information sharing and disaster recovery capabilities. Also, the Department matured key information technology management functions, such as portfolio management. However, challenges remain to recruit people with the necessary skills to perform certain management functions. Budget review improvements are needed to enable the Chief Information Officer to identify and resolve issues before component investments are finalized.

We are recommending that that the Deputy Under Secretary for Management assign the Chief Information Officer a key role in the Department's information technology budget planning process.

Background

The Homeland Security Act of 2002, as amended, established the position of the DHS Chief Information Officer (CIO) to govern information technology (IT) across 22 component agencies to ensure that technologies and services are in place to meet DHS' mission needs. The primary mission of the DHS CIO is to lead, govern, integrate, and manage IT functions throughout the Department.

The component agencies that make up DHS rely heavily on IT to perform a wide range of mission operations, including counterterrorism, border security, and emergency response, among others. To support its mission operations, DHS had an IT budget of approximately $6 billion for fiscal year (FY) 2011. This represents nearly 14 percent of the DHS overall budget of $43.6 billion. Given the size and significance of this investment in IT, effective management of IT programs and expenditures is critical. Figure 1 includes IT budgets for the seven operational components of DHS: U.S. Customs and Border Protection (CBP), Transportation Security Administration (TSA), United States Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE), United States Coast Guard (USCG), Federal Emergency Management Agency (FEMA), and United States Secret Service (USSS).

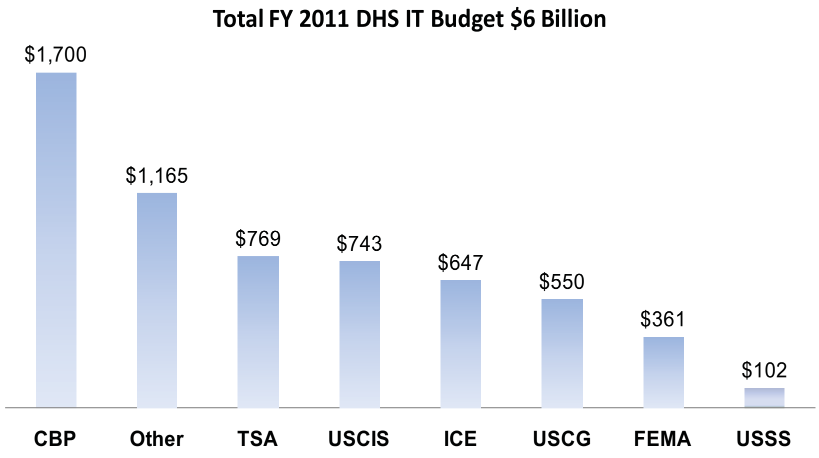


Figure 1: Component IT Budgets FY 2011 (in millions)

The DHS CIO reports to the Under Secretary for Management and is supported by the Office of the CIO (OCIO), which is composed of the CIO, a Deputy CIO, a Chief of Staff, and approximately 344 Federal staff. The OCIO administers the Department's IT infrastructure, applications, services, and management functions. The mission of the OCIO is to ensure that more than 220,600 DHS employees remain connected to the Department's IT infrastructure environment and to ensure operational excellence. Figure 2 shows the organization chart of the six OCIO offices.

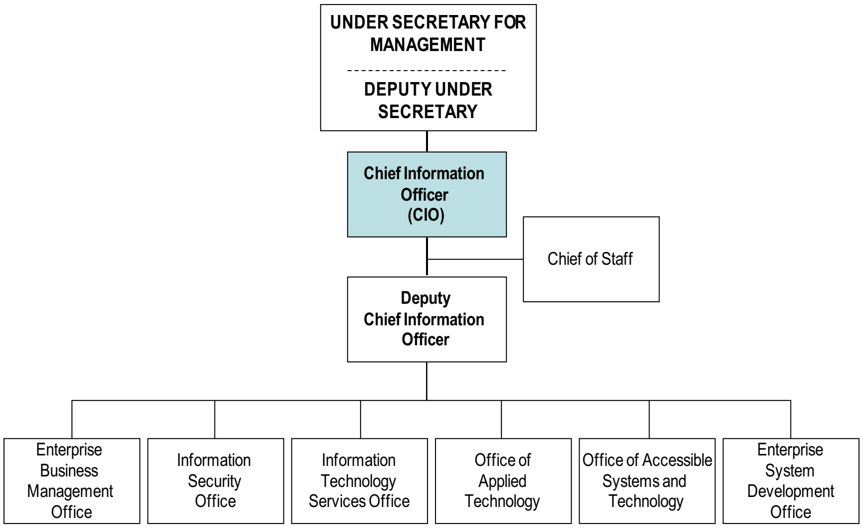

UNDER SECRETARY FOR MANAGEMENT
DEPUTY UNDER SECRETARY
Chief Information Officer (CIO)
Chief of Staff
Deputy Chief Information Officer
Enterprise Business Management Office
Information Security Office
Information Technology Services Office
Office of Applied Technology
Office of Accessible Systems and Technology
Enterprise System Development Office

Figure 2: DHS OCIO Organization Chart

The Enterprise Business Management Office (EBMO) oversees IT budget functions and ensures that the Department's IT investments align with its missions and objectives. 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 mission needs and regulatory requirements. The Information Technology Services Office is responsible for managing the IT infrastructure, including network, email, Internet, telecommunications infrastructure, and end-user services, in accordance with the Department's mission and goals. The Office of Applied Technology has primary responsibility for the Department's enterprise architecture, data, technology, and governance services. The Office of Accessible Systems and Technology leads Department-wide implementation of Section 508 of the *Rehabilitation Act of 1973*,[1] as amended, providing technical support and training to ensure that employees and customers with disabilities have equal access to information and data. Finally, the Enterprise System Development Office provides enterprise IT services, such as Microsoft SharePoint, for DHS customers.

[1] 29 U.S.C. Section 794d.

The DHS CIO is responsible for all IT programs in the Department and provides leadership to support the Department's vision for "One Network, One Infrastructure, One DHS." In 2005, the Department began to modernize and integrate critical IT functions and systems to establish "one infrastructure" for improved information sharing across components. To achieve this goal, the Infrastructure Transformation Program was established, representing the Department's full-scale move toward a DHS-wide consolidated IT infrastructure. This program comprises a group of interrelated initiatives, listed below, designed to generate a more robust and cost-effective infrastructure for the Department.

Data Center Consolidation

This project's strategic vision is to reduce the number of existing component data centers to two secure, geographically separate enterprise data centers to minimize infrastructure while enhancing the Department's disaster recovery posture. These two enterprise data centers became operational in 2008.

OneNet

In 2005, the Department began to consolidate and transform its individual component networks into a single wide area network, known as OneNet. The Department's goal for OneNet is to facilitate the ability of all DHS components to share data. The completed OneNet will provide a centralized Network Operations Center and Security Operations Center to achieve cost effectiveness and improve security by reducing the number of trusted Internet connections. OneNet received its original authority to operate in May 2005.

Email and Collaboration Services

The OCIO offers email services as part of an effort to standardize email platforms, addressing, and naming conventions across the Department. The OCIO also offers collaboration services, such as Microsoft SharePoint, to promote information sharing across the Department. Once implemented, these offerings should improve service levels and redundancy at a reduced cost. The DHS OCIO expects to have more than 100,000 users DHS-wide on the email service offering by the end of FY 2012.

Creating a management structure for effective oversight and strategic management of Department-wide IT assets and programs has been a major challenge for the Department. In 2004, we reported that the DHS CIO had a significant role in guiding IT resources and capabilities to fulfill the Department's diverse missions.[2] However, despite being tasked with DHS-wide IT responsibilities, the CIO was not a member of the senior management team. Also, there was no formal reporting relationship between the DHS CIO and the CIOs of major component organizations. We recommended that DHS implement plans for centralizing IT, reposition the CIO to report directly to the Deputy Secretary, document and communicate the roles of component-level CIOs, provide the DHS OCIO with adequate staff resources, and have component-level CIOs report to both the DHS CIO and their respective agency heads.

In 2008, we reported that DHS had made progress to improve the CIO's oversight of IT acquisitions.[3] However, major challenges remained. These challenges included continued OCIO staffing shortages, insufficient implementation of component-level management practices, and unmet goals in IT infrastructure consolidation. We recommended that the DHS CIO augment the DHS OCIO Staffing Plan to include specific actions and milestones for recruiting and retaining full-time employees. We also recommended that the DHS CIO ensure that component CIOs (1) submit comprehensive, standardized IT budgets to the DHS CIO and (2) develop and maintain IT strategic plans and enterprise architectures that align with those of DHS.

Federal Agency CIO Benchmarking

We met with senior officials from five Federal agencies to discuss how, based on Federal guidelines, they structured their IT organizations to administer centralized management of IT to support mission needs. We met with the Department of Energy (DOE), Department of Justice (DOJ), Department of Health and Human Services (HHS), Department of Agriculture (USDA), and the Department of Veterans Affairs (VA). These agencies were selected based on size or complexity comparable to DHS. We met with the CIOs of these agencies to discuss organizational structure, IT processes, policies, and procedures used to administer agency-wide IT management. Table 1 summarizes this information in comparison with DHS.

[2] *Improvements Needed to DHS' Information Technology Management Structure* (OIG-04-30), July 2004.
[3] *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG-08-91), September 2008.

Table 1: Comparison of DHS and Federal Agency CIOs

	Reports to the Agency Head	Total Agency Staff (Federal)	Full-time Federal IT Staff Under CIO Control	FY 11 Total IT Budget ($ Billion)	CIO Controls IT Spending Agency-wide	Standard IT Lifecycle Mgmt Approach	▲
DHS	N	220,600	344	6	N	Y	6.1
DOE	Y	16,000	144	2	Y	Y	9.1
DOJ	N	112,000	289	3	N	Y	6.9
HHS	N	73,000	94	7.2	N	Y	6.7
USDA	N	120,000	1,056	2.5	Y	Y	8.1
VA	Y	294,000	7,234	3.7	Y	Y	4.8

▲"Federal IT Dashboard Rating (as of October 2011)"

Similar to DHS, three of the other five Federal CIOs do not report directly to their agency heads. However, the CIOs at the three agencies said that there is adequate opportunity to advise and influence leadership on agency-wide IT matters. The number of IT staff under the VA CIO's control is considerably larger than the other five agencies. This is due, in part, to a 2006 realignment of all IT personnel to the CIO. With regard to IT budgets, HHS has the largest investment in IT at $7.2 billion; however, $3.25 billion of this is assigned for State grants. Three of the six CIOs claimed to have oversight and authority of agency-wide IT investments. The remaining three CIOs said that they do have some degree of influence over existing agency-wide IT investment review processes through investment review boards or other decision making bodies. All CIOs said that they had a standard IT life cycle management approach in place to ensure consistency across IT programs. Finally, all agencies have received a rating from the Federal IT Dashboard, which reflects the agency CIO evaluation, cost, and schedule for each investment.

Results of Audit

Progress Made To Establish CIO Oversight and Authority

DHS has made progress in increasing DHS CIO oversight and authority of Department-wide IT programs and assets. Specifically, the OCIO has increased oversight of IT programs by conducting annual IT program reviews and implementing a new process to conduct in-depth reviews of selected IT programs. In addition, the DHS CIO has increased oversight of IT software, hardware, and infrastructure purchases through the IT acquisitions review process. Further, the Department has taken steps to better define the DHS CIO role. Increased CIO oversight and authority has resulted in better visibility of IT investments and programs, thus enabling the CIO to make strategic recommendations for reducing costs and duplication across the Department's IT environment.

DHS CIO Has Established Formal Oversight of IT Programs

The *Clinger-Cohen Act of 1996*,[4] as amended, gives the CIO responsibility for advising the agency head on whether IT programs and projects should be continued, modified, or terminated. The Federal CIO's IT reform plan[5] requires agency CIOs to implement initiatives to improve management of large-scale IT programs. For example, agency CIOs must lead a series of reviews, known as TechStat sessions, for selected IT investments in order to identify program performance issues and recommend corrective actions. In addition, Office of Management and Budget (OMB) Memorandum M-11-29[6] states that agency CIOs have responsibility for the agency's entire IT portfolio. DHS Management Directive (MD) 0007.1[7] defines such roles and responsibilities of the DHS CIO as conducting program reviews, recommending program improvements or corrective actions, and providing the Office of the Secretary and component heads with an annual evaluation of IT program performance.

The OCIO has increased its oversight of IT investments by establishing a formal process to conduct annual reviews of IT programs. In addition, the OCIO has adopted the TechStat process

[4] Public Law 104-106, Division E, Section 5125, February 10, 1996. The law, initially titled the Information Technology Management Reform Act, was renamed the Clinger-Cohen Act of 1996 in Pub. L. 104-208, September 30, 1996.

[5] The *25 Point Implementation Plan To Reform Federal Information Technology Management*, December 9, 2010.

[6] OMB M-11-29, *Chief Information Officer Authorities*, August 8, 2011.

[7] Department of Homeland Security, Management Directive 0007.1, *Information Technology Integration and Management*, March 15, 2007.

to conduct more in-depth reviews for a selection of major IT programs.

Annual IT Program Reviews

The OCIO has established a process to conduct annual reviews of IT programs and to improve accountability and visibility of program performance (see figure 3). Program reviews are facilitated by EBMO's Program Governance Division and include all major IT investments. EBMO personnel review program documentation, such as OMB Exhibit 300s and previous acquisition or program assessments, to evaluate performance and issue ratings. The OCIO conducted reviews for 79 major IT programs in FY 2010 and 48 additional IT programs in FY 2011.

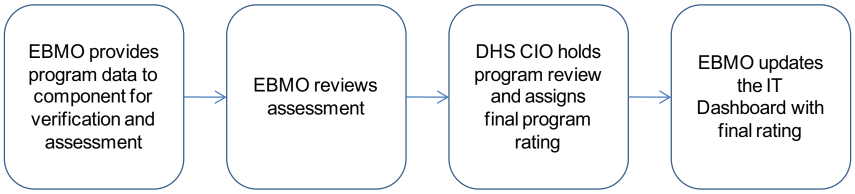

EBMO provides program data to component for verification and assessment
EBMO reviews assessment
DHS CIO holds program review and assigns final program rating
EBMO updates the IT Dashboard with final rating

Figure 3: OCIO Program Review Process

These reviews also meet OMB's requirement for CIOs to rate programs in the areas of cost, schedule, and performance and provide updates to the Federal IT Dashboard.[8] EBMO personnel work with IT program stakeholders, including component CIOs, DHS capital planning personnel, and component program managers, to reach agreement on each program rating using pre-established criteria. As of November 2011, the Federal IT Dashboard included ratings for approximately 800 major investments. DHS' overall rating was 6.1 (out of 10) for a combined 87 major IT investments.

The CIO also uses information from the reviews to identify issues and develop specific recommendations for improving program cost, schedule, and performance. At the time of our review, the OCIO had issued 90 recommendations to the Deputy Secretary for the 2013 budget year. Specifically, the CIO recommended that 81 IT investments continue as planned, eight investments be continued but modified, and one be suspended. For example, the CIO recommended a budget modification to reinstate $10 million in funding per year for the CBP Traveler Enforcement Compliance

[8] In June 2009, OMB released a public website known as the Federal IT Dashboard to improve the transparency and oversight of agencies' IT investments.

System Modernization in order to prevent further schedule delays. The CIO also recommended that FEMA suspend work on its National Flood Insurance Program Information Technology Systems and Services until business requirements were better defined.

In-Depth IT Program Reviews

The DHS OCIO further improved its IT program reviews by adopting the TechStat process and criteria, which enables a deep analysis of select IT programs. In 2011, EBMO established a TechStat Management Office to conduct reviews of selected high priority or high-risk IT investments that received low ratings in previous reviews. The TechStat Management Office conducts an in-depth analysis of program data and interviews stakeholders to determine the status of a program and the reasons for any problems identified. The TechStat process is illustrated in figure 4.

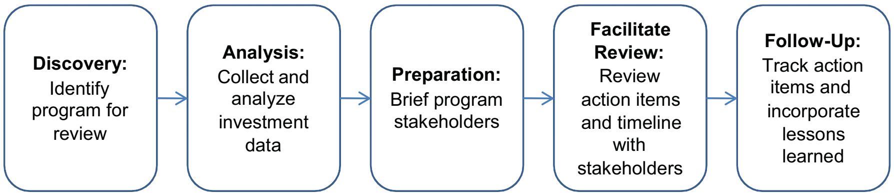

Discovery: Identify program for review
Analysis: Collect and analyze investment data
Preparation: Brief program stakeholders
Facilitate Review: Review action items and timeline with stakeholders
Follow-Up: Track action items and incorporate lessons learned

Figure 4: OCIO TechStat Process

As of August 2011, the OCIO had completed two TechStat reviews: the Student and Exchange Visitor Information System II and the DHS Infrastructure Transformation Program. Based on the results of these reviews, the OCIO made 13 recommendations to senior leadership and program managers to address challenges identified, such as program governance and staffing. For example, the OCIO TechStat Infrastructure Transformation Program review team recommended the establishment of an Executive Steering Committee consisting of senior-level stakeholders to ensure delivery of capabilities. At the time of our audit, 24 abbreviated TechStat reviews were completed or in progress.

DHS CIO Has Increased Oversight of IT Acquisitions

The *Clinger-Cohen Act* assigns the CIO responsibility for ensuring effective acquisition of IT resources. In addition, DHS MD 0007.1 states that the DHS CIO is responsible for reviewing and approving IT acquisitions over $2.5 million.

The DHS CIO maintains oversight of IT software, hardware, and infrastructure purchases through routine reviews of all IT acquisitions over $2.5 million. Since our 2008 report, EBMO has established a dedicated IT Acquisition Review Branch to administer these reviews. The review allows the OCIO to verify compliance with technical standards, regulations, and alignment with DHS strategic goals and objectives.

The volume of IT acquisition reviews has increased from 243 in FY 2007 to 387 in FY 2011. The number of approvals for IT acquisition requests has increased from 129 in FY 2007 to 311 in FY 2011. Figure 5 shows the number of IT acquisition requests submitted and reviewed and the number of requests approved from FY 2007 through FY 2011.

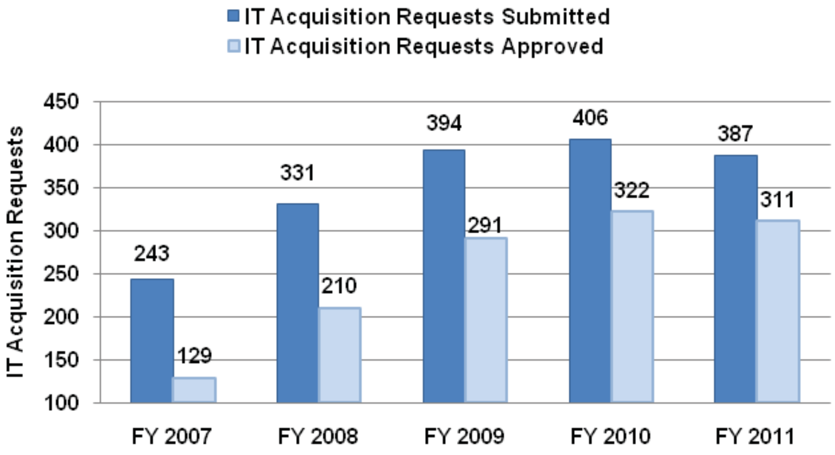


Figure 5: DHS IT Acquisition Reviews FY 2007–2011

EBMO is also taking steps to improve the IT acquisition process. In FY 2010, EBMO established a goal to process IT acquisitions within 10 business days. However, this goal was not met. Some IT acquisition reviews took up to 38 days. To address this situation, the IT Acquisition Review Branch will be making significant changes to streamline the component data required and refine the review procedures. For example, EBMO is working to reduce the number of questions the components must answer when preparing a request by 50 percent. EBMO also plans to increase efficiency by automating the review process using a web application. These efforts should reduce overall processing time and improve tracking capabilities for the entire Department. Additional planned enhancements to reduce the processing time include distinguishing between IT acquisitions that need to complete the entire review process and those that need to complete only certain steps.

DHS CIO Responsibilities and Authority Are Better Defined

OMB M-11-29 clarifies the primary area of responsibility for agency CIOs. Specifically, agency CIOs must drive the investment review process for IT investments and have responsibility for the entire IT portfolio, focus on eliminating duplication in their agency's IT investments, improve the overall management of large IT projects, and have the authority and responsibility to provide information security for the agency.

DHS has taken action to better define the CIO's authority and responsibility. Specifically, the DHS Deputy Secretary, in a May 2011 memorandum,[9] directed the CIO to take a greater role in the review and execution of all IT infrastructure investments. To formalize this guidance, the DHS Undersecretary for Management began an effort to update the Delegation of Authority for the DHS CIO. As of October 2011, the OCIO was incorporating revisions from the DHS CIO and component CIOs in the revised draft delegation.

The increased oversight of IT investments gained through the IT program, TechStat, and acquisition reviews has provided the DHS CIO with better visibility of Department-wide IT programs and assets. The CIO has a central vantage point for IT capabilities that perform similar functions or support mission needs. This expanded visibility has enabled the CIO to identify opportunities for reducing costs and duplication across the Department's IT environment. For example, the OCIO's Enterprise Architecture Office conducted a review of information sharing IT capabilities and identified approximately 14 network portals that can be consolidated within the Homeland Security Information Network by FY 2013. The Enterprise Architecture Office recommended that the Information Sharing Portfolio Governance Board consolidate network portals to improve alignment with the enterprise architecture. The OCIO expects to save at least $42 million over the next five years from this effort.

The CIO has made additional recommendations to the Deputy Secretary to reduce IT infrastructure duplication through program reviews. For example, the CIO recommended that the National Protection and Programs Directorate evaluate opportunities to collaborate and leverage screening services and capabilities across components as part of its ongoing IT infrastructure program. The

[9] DHS Deputy Secretary, *Information Technology Efficiency*, May 5, 2011.

OCIO is also planning to improve efficiencies by leveraging watchlist service capabilities between the Terrorist Screening Center and CBP to enable real-time updates of the Terrorist Screening Database. Likewise, the OCIO recommended a Department-wide repository for all biometric data that can be leveraged by multiple component systems.

Finally, OCIO management officials said that TechStat reviews have provided additional opportunities for the CIO to issue corrective actions for programs. For example, the OCIO's TechStat Office reviewed the Student and Exchange Visitor Information System II after the program did not meet its schedule in 2009. The Student and Exchange Visitor Information System II is a database and reporting system for tracking the visa status of nonimmigrant students and exchange visitors to the United States. Upon review, the TechStat team determined that the program lacked effective governance to control scope changes and make decisions, had inadequate staff resources to provide critical program services, and was not leveraging DHS enterprise customer account services. The TechStat Office recommended a new governance structure, further evaluation of staff to ensure appropriate staffing levels and capabilities, and inclusion in an enterprise-wide solution for customer account service.

Progress Made Toward IT Integration

DHS has taken steps toward achieving its Department-wide IT infrastructure integration goals. Specifically, the OCIO has met a number of milestones to consolidate data centers across the Department, integrate disparate component networks into a single DHS network, and create centralized email and collaboration services to improve information sharing. Progress has been leadership driven through the communication of Department-wide IT efficiency goals and priorities. The CIO has reiterated these goals by establishing high-priority initiatives that hold components accountable for completing consolidation efforts. Once completed, the Department expects that IT integration will result in improved disaster recovery capabilities, cost savings, and increased information sharing.

Data Center Consolidation Efforts Underway

The *Paperwork Reduction Act of 1995* and the *Clinger-Cohen Act of 1996* require agencies to ensure that IT is acquired, used, and managed to improve performance of agency missions. In addition, DHS MD 0007.1 requires the DHS CIO to direct the consolidation and optimization of DHS IT infrastructure equipment, services, people, and processes to improve IT interoperability and value in support of the DHS mission.

The OCIO has taken a number of steps to consolidate component data centers. In the past, 43 separate computing sites supported the DHS components. The OCIO IT Services Office is coordinating and overseeing the provision of facility space and services for components at the two DHS enterprise data centers. The enterprise data centers, located in Mississippi and Virginia, are large-scale, physically secure facilities that offer various services and disaster recovery capabilities not previously available to some components.

To accomplish the consolidation, each component will transfer its systems and services from existing sites to one of the two enterprise data centers or to a virtual space supported by the data centers. Once the transfer is complete, the enterprise data center assumes the operation of systems and services, and the component data centers are shut down. As of November 2011, DHS headquarters, FEMA, TSA, and CBP had migrated some applications from eight sites to a DHS enterprise data center. The transfer of operations from three additional sites to the enterprise data centers was to be completed by the end of 2011. Table 1 lists the component data centers that consolidated or were scheduled to consolidate with the enterprise data centers by the end of 2011.

Table 2: Enterprise Data Center Consolidation Efforts

Completed consolidation as of November 2011	Due to complete consolidation by end of 2011
1. CBP – Commercial Recovery Facility	1. ICE/USCIS/United States Visitor and Immigration Status Indicator Technology – Dallas site
2. CBP – Tysons site	2. ICE/USCIS/ United States Visitor and Immigration Status Indicator Technology – Rockville site
3. FEMA – N. Virginia Commercial Data Center	3. FEMA – Plano site
4. TSA – IBM St. Louis Hosting Center	
5. TSA – Headquarters site	
6. DHS – Ashburn Center	
7. DHS – Stafford Center	
8. DHS – HSDN Fair Lakes	

All 43 component sites are projected to complete major migration activity, such as transferring hardware and consolidating and moving legacy systems, applications, and data, by the end of FY 2014. However, OCIO officials said that funding uncertainty could delay the completion of data center migration until FY 2015.

Although DHS has made progress toward consolidating data centers, until migration is complete, the Department will incur significant costs for unoccupied space at the two enterprise data centers. In FY 2011, the Department paid more than $55 million for unused space at the centers. The Department incurred this cost even though the first enterprise data center had reached 75.5% occupancy and the second data center had reached 56.4% occupancy as of July 2011.

Component IT Network Consolidation Advances

In addition to the consolidation of data centers, the OCIO has taken steps to consolidate existing individual component networks into one integrated network—DHS OneNet. Specifically, DHS has established an enterprise OneNet backbone, as well as a primary and secondary network operations center and security operations center. Seven major components[10] have signed up to receive network and security services from OneNet. As of November 2011, five of the seven components were connected to OneNet.

[10] The seven major components are CBP, FEMA, ICE, TSA, USCIS, USCG, and USSS.

These components are able to access the Internet through OneNet's Trusted Internet Connection.[11] In addition, progress has been made to establish a connection to both enterprise data centers and to begin network security enhancements.

Additional steps are required to ensure complete connectivity to OneNet. Specifically, all DHS components must be connected to OneNet in order for each component's transition to be complete. However, at the time of our audit, only two components had connected all sites to OneNet. To complete this step, components are dependent on DHS' implementation of the necessary security for information sharing among the components. The OCIO is working on expanding the OneNet infrastructure to accommodate component-based security policies to enable all components to connect existing sites to the DHS network. DHS plans to complete the migration to OneNet by December 2013.

Enterprise IT Service Offerings Created

The OCIO has begun offering centralized IT services housed at the two enterprise data centers, such as email and Microsoft SharePoint, to foster communication among components and achieve economic savings through consolidation. As of November 2011, one component has subscribed to receive email services and two additional components are testing the service. The email service provides subscribers with a global address book and collaboration capabilities, such as meeting scheduling and shared calendars. In addition, three components have signed up to use the SharePoint service. This service is expected to increase collaboration between components through the use of a web-based application that allows teams to work together on projects.

Additional efforts to improve information sharing include the development of an information sharing environment, which is a formal partnership among all levels of government, the private sector, and foreign partners for facilitating access to information to prevent future terrorist attacks. For this effort, the DHS OCIO established an Information Sharing Environment Office in August 2011 to provide oversight and management for related programs, such as the Common Operating Picture Program. The Common Operating Picture Program provides analysis and storage of information, improving situational awareness of potential threats to the Nation's infrastructure. The OCIO plans to complete an

[11] The Trusted Internet Connection initiative improves network security and incident response by reducing and consolidating the number of external connections.

upgrade of the Common Operating Picture Program in 2012, which will include a centralized process for requesting information within DHS. Plans are also underway to make this program available to external partners. In addition, the OCIO's Information Sharing Environment Office participates in the National Information Exchange Model, a collaborative effort to increase information sharing among DHS, DOJ, HHS, and State, local, and private stakeholders. Specifically, the National Information Exchange Model establishes a framework with a common vocabulary to improve sharing of intelligence. DHS is working to institutionalize these information sharing initiatives.

IT Efficiency Goals and Priorities Established and Communicated

The Department has been working to consolidate and integrate component systems and hardware since 2003, but DHS components have not always embraced these efforts. To address this situation, Department leadership established IT efficiency goals and priorities. For example, the Deputy Secretary identified the advancement of operational efficiency for IT capabilities as a Department-wide goal.

In addition, the DHS CIO made IT integration a top priority for component CIOs in 2010 by including it on the Department's high priority IT initiatives list. The DHS CIO and the component CIOs have agreed to include the transition to DHS OneNet and enterprise data centers as formalized high priority initiatives for FY 2011. For example, High Priority Initiative number 11-33, documented in the OCIO's FY 2011–2015 IT Strategic Plan, states that DHS will continue management of components' migration to enterprise data centers. Component project managers are required to report on progress for both data center and OneNet migration efforts by updating a tracking tool that creates monthly status reports. These updates, which are provided to the component CIOs, demonstrate whether milestones have been met, and if not, why they have not been met.

The DHS CIO has effectively communicated the goals for achieving IT integration across the Department to the components through numerous OCIO outreach efforts. For example, the DHS CIO outlined the next steps for DHS IT infrastructure consolidation in a 2011 memorandum[12] to the Department. This memorandum

[12] DHS CIO, *Next Steps in IT Infrastructure Rationalization and the DHS Data Center Consolidation Strategy*, August 12, 2011.

also included requirements that components move to both email and collaboration services. Additionally, the DHS CIO uses the CIO Council to communicate goals and objectives for achieving Department-wide IT integration. The OCIO has also created several documents to further explain and promote the different aspects of Department-wide integration, including data center migration and OneNet, and made them available on its website. For example, a Data Center Migration Customer Guide provides an overview of the migration process, including the costs and benefits. Also, the OCIO provides components with a service catalog that lists the different Department-wide services being offered. Finally, OCIO representatives have visited components to present a complete overview of the different service offerings.

Integration Benefits Being Realized

The Department is starting to realize the benefits of its integration efforts. Specifically, the components that have transferred operations to the enterprise data centers have enhanced disaster recovery capabilities. The two enterprise data centers are equipped with redundant facilities and services and are in geographically dispersed locations. In addition, both data centers offer remote management solutions and continuity of operations in the event of a disaster.

Some components are also realizing cost savings from the data center consolidation and enterprise services. Specifically, the consolidation of the Department's data centers alleviates components' costs for building and maintaining individual data center facilities. Although components moving to the data centers must pay certain fees,[13] OCIO IT Services Office officials said that components eliminate the costs of maintaining individual legacy data center facilities, which results in savings for some components. For example, TSA is saving more than $8 million annually in reduced operations costs after moving its primary systems from Missouri to the enterprise data centers.

Subscribing to DHS' enterprise IT service offerings has also resulted in cost savings. For example, FEMA is saving on annual costs by transitioning its existing email service to the enterprise email service hosted in the DHS enterprise data center. Using the email service reduced the cost of FEMA's individual email mailboxes from $300 each to $29 each. Additional benefits were

[13] Components migrating to the DHS enterprise data centers pay a one-time charge, a technical service charge for operations and maintenance, and an annual charge for space used.

gained as FEMA was able to reduce the number of dedicated IT staff working on email from eight to two. In addition, FEMA IT officials said the enterprise email service included hardware upgrades and improved email capabilities, such as increased capacity and dynamic archiving.

The Department's transition to enterprise-level networks and services is improving collaboration and information sharing. Specifically, DHS is offering access to OneNet for Federal, State, local, and tribal governments, and provides gateways for data exchange between DHS and other networks, including the Department of Defense. The enterprise-wide services, such as SharePoint, also increase collaboration and information sharing by providing users with basic and custom sites to work with team members on projects. Finally, the Information Sharing Environment Office's upgrade of the DHS Common Operating Picture Program and increased use of the National Information Exchange Model are expected to improve access to information to help prevent future terrorist attacks. An upgraded Common Operating Picture Program will be completed in 2012, which will include the deployment of a centralized request for information process within DHS. Further, the National Information Exchange Model is implementing a strategy for increasing implementation of the program throughout all areas of State and local government.

Progress Made To Advance IT Management Functions, But Further Improvements Are Needed

DHS has made progress in improving IT management functions since our audit in 2008. Specifically, the OCIO has taken steps to mature key IT management functions and to ensure that they are carried out in an integrated fashion to improve CIO decision making. These improvements are due to an increase in OCIO staffing levels, organizational restructuring, and better collaboration among component CIOs. However, challenges remain to recruit people with the right skill sets to perform certain IT management functions. Further, other challenges remain to improve the effectiveness of the CIO's current IT budget review process to enable the CIO to identify and remediate issues before IT investments are finalized.

Progress Made To Improve IT Management Functions

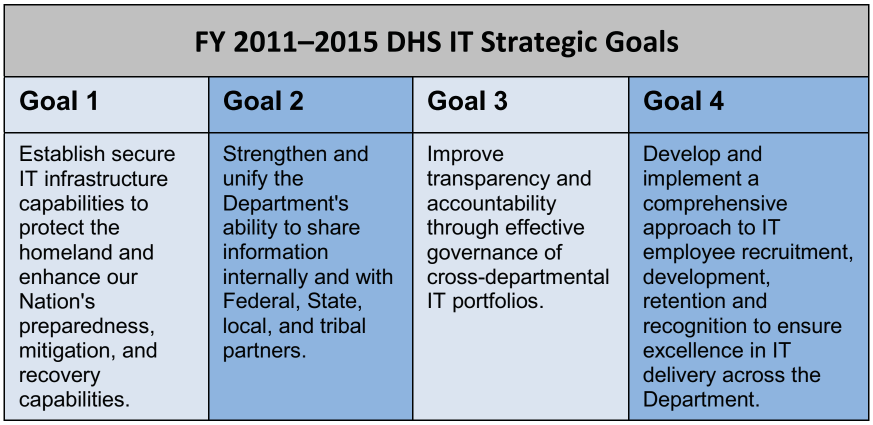
The *Clinger-Cohen Act of 1996* requires that Federal departments and agencies establish CIOs to institute, guide, and oversee frameworks for managing IT Department-wide. Additionally, DHS MD 0007.1 gives the CIO the responsibility to lead, govern, integrate, and manage IT functions throughout the Department.

The OCIO has made progress in improving IT management functions since our review in 2008. Specifically, it has taken steps to mature key management practices, such as strategic planning, Capital Planning and Investment Control (CPIC), enterprise architecture, portfolio management, and IT budget reviews.

Strategic Planning

The *Government Performance and Results Act* holds Federal agencies responsible for strategic planning to ensure efficient and effective operations and use of resources to achieve mission results.[14] In addition, DHS MD 0007.1 states that CIOs are responsible for developing and implementing a detailed IT strategic plan. The OCIO developed an IT strategic plan for FY 2011–2015 that includes a clear vision, goals, and objectives to optimize the Department's IT infrastructure, applications, and services. The goals and priorities documented in the plan, and presented in figure 6, were vetted across all components to ensure collaboration and buy-in.

[14] PL 103-62, *Government Performance and Results Act of 1993*, August 3, 1993.



FY 2011–2015 DHS IT Strategic Goals			
Goal 1	**Goal 2**	**Goal 3**	**Goal 4**
Establish secure IT infrastructure capabilities to protect the homeland and enhance our Nation's preparedness, mitigation, and recovery capabilities.	Strengthen and unify the Department's ability to share information internally and with Federal, State, local, and tribal partners.	Improve transparency and accountability through effective governance of cross-departmental IT portfolios.	Develop and implement a comprehensive approach to IT employee recruitment, development, retention and recognition to ensure excellence in IT delivery across the Department.

Figure 6: DHS IT Strategic Goals

The OCIO has a process in place to update the IT strategic plan annually. The DHS CIO also facilitates an annual process with all component CIOs to select the OCIO's yearly high priority initiatives. These initiatives are included as an appendix to the IT strategic plan. As of November 2011, the OCIO was updating the IT strategic plan to include 30 FY 2012 high priority initiatives.

CPIC

OMB A-130 states that agencies must evaluate each IT investment to determine whether the investment will support mission functions.[15] DHS MD 4200.1 establishes a process for ensuring that IT investments support the agency's mission and business needs.[16] CPIC is DHS' primary process for making decisions about the systems in which the Department should invest. CPIC includes four cycles to plan, select, control, and evaluate IT investments in support of the annual budget cycle. In our 2008 audit, we reported that the DHS OCIO had established a process to ensure that IT investments have solid Exhibit 300 business case documentation pursuant to the annual OMB budget process.[17]

Since 2008, the OCIO has continued to execute its process to review Exhibit 300 business cases to effectively govern the four phases of the CPIC cycle. According to EBMO management, the process has remained consistent over the past several years, with minimal changes. Representatives from all components perform CPIC duties and belong to the OCIO's CPIC Administrators

[15] OMB Circular A-130, Revised, Management of Federal Information Resources.

[16] Department of Homeland Security, Management Directive 4200.1, IT Capital Planning and Investment Control (CPIC) and Portfolio Management.

[17] *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG-08-91), September 2008.

Group. The OCIO facilitates biweekly meetings for this group to provide guidance or discuss specific issues, as well as to answer questions from component representatives. EBMO published a new CPIC guide and communicated the guide to components in 2011 to ensure adherence to the current CPIC process.

Enterprise Architecture

The *Clinger-Cohen Act* charges CIOs with developing and maintaining an enterprise architecture. In our 2008 audit, we reported that the DHS OCIO had implemented an Enterprise Architecture Review Board to improve Department-wide IT management functions, such as reviewing and making recommendations to the DHS CIO for approving IT investments that are in line with the Department's mission and priorities.[18]

Since 2008, the OCIO has continued to execute Department-wide enterprise architecture efforts to drive IT development and decision making toward DHS mission needs. Specifically, the OCIO has established a Homeland Security Enterprise Architecture to define the current and future blueprint of Department-wide technology as it supports DHS' strategy and mission. The OCIO is using the Homeland Security Enterprise Architecture as a standard reference point to review investments for program alignment and technology decision requests. The OCIO has also established an Enterprise Architecture Program Management Office to advise DHS component agencies how to use the enterprise architecture to ensure that programs and IT initiatives are meeting Federal and departmental oversight and reporting requirements.

The OCIO has also piloted a process for developing segment architectures across DHS. Segment architecture development efforts are a business-driven process that establishes a detailed baseline architecture and transition plan for a particular segment of IT functions. The OCIO completed its first segment architecture for human capital functions in 2011. This effort provided the Department with a documented blueprint, which includes a comprehensive inventory of more than 400 human resources systems. Additional efforts are underway to define segment architectures for screening, IT infrastructure, and financial management capabilities.

[18] *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG-08-91), September 2008.

Portfolio Management

As part of the selection component of the capital planning process, OMB Circular A-130 requires agencies to prepare and maintain a portfolio of major IT systems that monitors investments and prevents redundancy of existing or shared IT capabilities. DHS MD 0007.1 establishes DHS policies and assigns responsibilities for managing IT investment using portfolio management, which involves developing groups of related DHS IT investments and assets. In 2008, we reported that the DHS OCIO had established 22 portfolios based on DHS mission areas, goals, and objectives to increase visibility of IT programs, projects, and systems.[19]

Since 2008, the DHS CIO has refined its approach to include functionally oriented portfolios for mission support and business functions. Specifically, the OCIO has identified 13 portfolios that group IT capabilities according to similar functions, such as the screening of individuals or incident response handling (see figure 7). The OCIO is conducting a pilot of three portfolios—Human Resources IT, Screening, and Information Sharing—as part of the FY 2012 budget cycle.

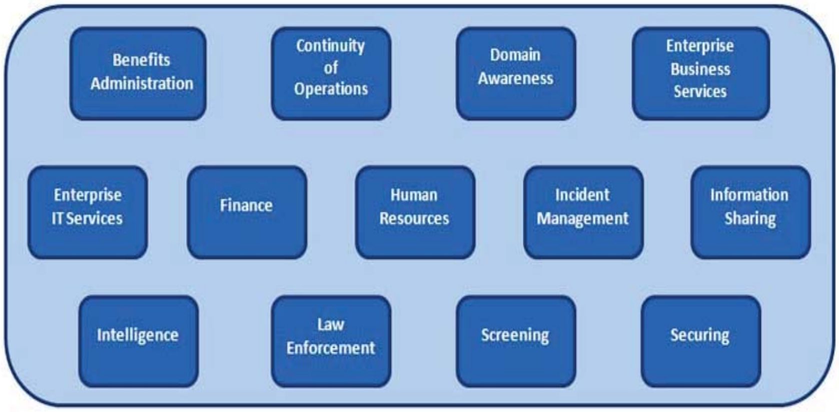


Figure 7: DHS Portfolios as of November 2011

The OCIO conducts an annual portfolio analysis to align IT investments with portfolios and identify redundancies or gaps. At the time of our audit, the OCIO had aligned more than 650 IT investments with the 13 portfolios. To perform this analysis, EBMO facilitates a portfolio review, with involvement from component CIOs, mission stakeholders, and DHS OCIO subject matter experts. Participants review IT investment data received

[19] *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG-08-91), September 2008.

from components during annual IT budget submissions, such as Capital Investment Plans. Findings from the portfolio analysis are provided to DHS executives and used as input for Program Review Board activities. The review conducted during the FY 2013 budget cycle marked the OCIO's second annual portfolio analysis.

As part of its overall portfolio management effort, the OCIO is establishing a portfolio-based governance structure, which will help it to integrate and streamline decision making. To do this, the OCIO has established an enterprise-wide governance model, which includes an integrated framework for governing the Department's IT investments within each functional portfolio. The model, pictured in figure 8, leverages portfolio management and enterprise architecture practices as well as existing governance boards in order to facilitate decision making.

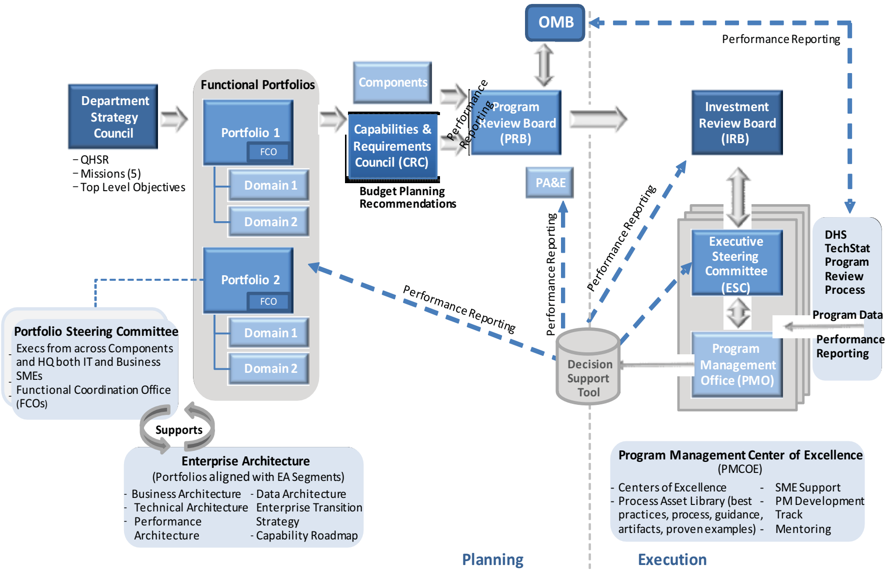

OMB
Performance Reporting
Department Strategy Council
- QHSR
- Missions (5)
- Top Level Objectives
Functional Portfolios
Portfolio 1
FCO
Domain 1
Domain 2
Portfolio 2
FCO
Domain 1
Domain 2
Components
Capabilities & Requirements Council (CRC)
Budget Planning Recommendations
Performance Reporting
Program Review Board (PRB)
PA&E
Investment Review Board (IRB)
Performance Reporting
Performance Reporting
Performance Reporting
Executive Steering Committee (ESC)
Program Management Office (PMO)
Decision Support Tool
DHS TechStat Program Review Process
Program Data
Performance Reporting
Portfolio Steering Committee
- Execs from across Components and HQ both IT and Business SMEs
- Functional Coordination Office (FCOs)
Supports
Enterprise Architecture
(Portfolios aligned with EA Segments)
- Business Architecture
- Technical Architecture
- Performance Architecture
- Data Architecture
Enterprise Transition Strategy
- Capability Roadmap
Program Management Center of Excellence (PMCOE)
- Centers of Excellence
- Process Asset Library (best practices, process, guidance, artifacts, proven examples)
- SME Support
- PM Development Track
- Mentoring
Planning
Execution

Figure 8: DHS Enterprise Governance Model, Draft

With this hierarchical governance structure, the OCIO plans to ensure that decisions are delegated to the appropriate governance level. Program-specific acquisitions decision events and enterprise architecture decisions are delegated to the appropriate portfolio or program-level governance board. The OCIO is in the early stages of piloting this governance model.

As part of the governance structure, the OCIO has implemented 14 executive steering committees to ensure collaboration and support from components to strategically govern investments. For example, a Human Resources Steering Committee was established in 2010. This committee includes membership from the OCIO, the DHS

Chief Human Capital Office, component CIOs, component Human Resources Directors, and the DHS Management Directorate. OCIO leadership said that this effort exemplified unprecedented Department-wide partnerships between the DHS Human Capital and IT communities.

The OCIO plans to further develop this new governance model as a framework to integrate portfolio management and enterprise architecture functions to improve alignment between IT assets, mission needs, and departmental strategy. The outcome of this process will include recommendations to the Program Review Board as to which investments to fund.

OCIO Organizational Improvements Made

IT management improvements are credited, in part, to the increase in OCIO's full-time staffing level, organizational restructuring, and effective collaboration among component CIOs. In 2008, we reported that the DHS CIO was well positioned to manage IT resources, but was limited by insufficient staff resources to carry out the increasing IT management activities needed to support the Department.[20] Since that time, the OCIO has increased staffing significantly, from 71 full-time employees in 2008 to approximately 344 full-time employees in 2011. The OCIO plans to further expand its staffing level to nearly 450 by the fourth quarter of 2012. The OCIO staffing levels from 2008 to 2012 are depicted in figure 9.

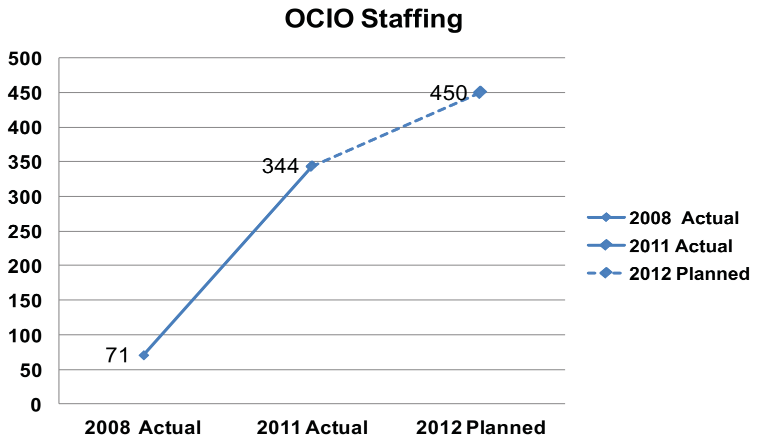


Figure 9: OCIO Staffing Levels as of October 2011

[20] *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG-08-91), September 2008.

Although the OCIO has increased its staff, finding people with the right skills to perform certain work, such as IT budget and portfolio reviews, remains a challenge. For example, there is only one full-time employee responsible for performing IT budget functions. This one employee conducted 75 percent of the portfolio review work for approximately 90 IT programs in FY 2010. The OCIO augments its staff by bringing in temporary assistance from other divisions or by coordinating with subject matter experts to conduct reviews. However, until offices such as EBMO are staffed sufficiently, budget and portfolio reviews may be hindered.

Additionally, the OCIO has restructured its six divisions to administer IT management practices more effectively. Specifically, EBMO was recently reorganized to establish a new Enterprise Portfolio Governance Division dedicated to executing portfolio reviews. This division provides support to portfolio stakeholders to administer portfolio activities, such as aligning programs with portfolios, creating baseline portfolios, and establishing portfolio pilot efforts. The OCIO also established a TechStat Management Office to conduct TechStat reviews. These offices are in the process of drafting a new concept of operations to reflect these new responsibilities.

Finally, the DHS OCIO improved communications and collaboration among component CIOs through biweekly CIO Council meetings. Component CIOs and Deputy CIOs told us that this forum provides an opportunity to communicate questions and issues to the DHS CIO and for the DHS CIO to communicate initiatives and priorities to the components.

Strategic Management of Department-wide IT

Specific IT management functions, such as portfolio reviews and enterprise architecture development, have enabled the DHS CIO to improve its strategic management of Department-wide IT assets and programs. Specifically, portfolio reviews have given the CIO visibility over the widespread challenges faced by many IT programs and the opportunity to recommend departmental improvements. For example, the CIO observed that many components are underinvesting in IT infrastructure and that the reuse and leveraging of IT systems and capabilities across components has not been optimized.

The portfolio reviews have also generated better visibility of specific IT systems and capabilities that can be consolidated. As part of the portfolio analysis work, the OCIO has identified more than 650 IT systems used to support similar functions. This information is further enhanced by progress to document segment architectures, which provides an inventory of processes, databases, and systems for each segment. As a result, the CIO is better able to conduct centralized management of IT within each portfolio, creating opportunities to recommend collaboration across components performing similar functions. For example, in 2011, a group of cross-component vetting subject matter experts performed a comprehensive review of Department-wide screening IT capabilities used to perform vetting functions. Currently, individual vetting checks are performed in more than 30 different systems across DHS with more than 100 unique business processes. The evaluation concluded with recommendations to centralize vetting services or leverage existing DHS services to reduce duplication of IT capabilities. Planning efforts are underway to leverage existing vetting data sources and improve automation among ICE, US-VISIT, and CBP. OCIO management told us that a DHS Vetting Executive Governance Board will be established to facilitate additional incremental enhancement to reach long-term enterprise solutions for vetting services.

The completion of segment architectures also provides the OCIO with a foundation for making better informed decisions to reduce redundancy and achieve cost savings. For example, the Human Capital Segment Architecture effort produced the Department's first human resources system inventory, which identified 422 systems and applications. Many of these systems are highly customized and suited for single use. As a result, the Human Resources IT Executive Steering Committee, a team of human resources and IT representatives, made approximately 50 recommendations to consolidate IT systems, integrate data repositories, and leverage existing IT platforms, among others. The DHS CIO said the Human Capital Segment Architecture will be a model for conducting segment architectures going forward. At the time of our review, the OCIO was working with the DHS Screening Coordination Office and DHS executives to establish the governance necessary to develop the Screening Segment Architecture.

Challenges Remain To Improve IT Budget Planning Practices

Although the DHS CIO reviews IT budgets submitted by components, early involvement in the components' IT budget planning process has been limited.

DHS MD 0007.1 assigns the CIO responsibility for reviewing and approving the DHS components' IT budgets.[21] In addition, this directive specifies that component CIOs are responsible for submitting IT budget to the DHS Chief Financial Officer (CFO) as part of the normal planning, programming, budgeting, and execution process.

The DHS OCIO Conducts a Comprehensive IT Budget Review

The DHS CIO conducts a review of all components' IT budgets as part of the DHS IT budget formulation process. To accomplish this, the OCIO uses the DHS CFO's Resource Allocation Plan (RAP) process to solicit IT budgets from each component. OCIO IT Budget Office personnel review component capital investment plans and supporting documents to confirm alignment of each investment with strategic goals and portfolios. The Budget Office also checks IT investments to confirm alignment with high priority departmental initiatives and plans for implementing the IT Reform Plan. Table 3 depicts the existing budget review process.

Table 3: DHS OCIO IT Budget Review Process

❖ Components submit resource allocation plans in spring (includes 5-year resource plan)
❖ CIO conducts review of IT resource allocation plans ❖ EBMO's Performance Management Division conducts an IT-focused analysis of the RAP submissions ➢ Analyze and consolidate information for the component ➢ Conduct review with component or DHS headquarters unit ➢ Consolidate financial performance data for inclusion in DHS CIO performance report "package" ➢ Record DHS CIO questions and/or decisions taken for follow up, monitoring, and status reporting
❖ Draft resource allocation decisions issued to components
❖ Components have the opportunity to appeal decisions
❖ Secretary and Deputy Secretary make final decisions
❖ Final resource allocation decision issued; defines the budget and future years Homeland Security program for submission to OMB

The IT budget review results are compiled into an executive briefing, which includes analysis and findings from the budget review as well as the portfolio reviews. The results include a set of CIO recommendations, by portfolio, that are used to support the

[21] DHS MD 0007.1 requires the DHS CIO to submit IT budget submissions to the DHS CFO as part of the annual Planning, Programming, Budgeting and Execution process.

CFO and DHS leadership in the program and budget review decision making process. Together, these reviews are essential for the DHS CIO's visibility of the IT budget across DHS in order to remediate IT budget issues before submitting the budget to OMB.

The IT budget reviews have provided the CIO with insight into each component's IT spending plans. For example, a review of one component's IT budget revealed a funding request for approximately $6 million to improve IT infrastructure. However, the OCIO had requested $91 million from the component for data center migration costs for the same budget year, highlighting a discrepancy in funding plans. OCIO management officials said that although the IT budget reviews are useful to confirm that component plans are in line with departmental priorities, they are not effective for changing existing component IT spending plans.

The CIO Is Not Adequately Involved in IT Budget Planning

Although the Department has given the CIO authority over IT spending, challenges remain for the CIO to affect budget decisions. Specifically, the CIO is not involved in and thus cannot provide input during the component IT budget planning process. To obtain funding for new initiatives, initial planning activities begin in the previous fiscal year during the budgetary planning phase. These planning steps are completed prior to the Department's budget programming phase. The CFO RAP process takes place after components have completed their planning for specific IT initiatives. Therefore, the CIO IT budget reviews do not directly affect the amount of funding components receive. As a result, components can obtain funding for IT investments regardless of the decisions made during the budget review process.

Additional challenges arise when components submit incomplete IT budget data, preventing the OCIO from performing meaningful analysis of budget plans. According to EBMO management, component budget submissions often lack detail or include irrelevant and out-of-date information. For example, as part of the budget review process for FY 2010, one component submitted requests for more than $250 million without providing the OCIO with sufficient information on the funds' specific purpose. In the same fiscal year, another component failed to include information on important milestones for more than half a dozen initiatives. The lack of quality data also affects other important OCIO management functions, such as portfolio reviews, which rely on the same component budget documentation.

The combination of the CIO's exclusion from the early budget planning stages and missing or poor component budget information limits the CIO's ability to make meaningful decisions and recommendations. Without earlier insight into and review of IT budget planning, the CIO cannot ensure that component IT budget plans are in alignment with departmental IT goals and objectives. Additionally, delayed inclusion in the planning process limits the CIO's ability to remediate IT budget issues prior to their formal submission to OMB as part of the Homeland Security budget.

Other Federal agencies experience similar challenges. Three of the five external Federal agency IT officials with whom we met faced similar problems with the budget process. These problems included issues with budget execution, limited oversight, a lack of real enforcement capability, and the need for better visibility and oversight. For example, one Federal CIO told us that enforcing budget authority presents organizational challenges, forcing this official to rely on the Secretary for enforcement support. Another Federal IT official voiced similar concerns with the CIO's inability to veto potential problem programs.

VA officials told us that they have been successful in addressing these issues through a combination of new policy and organizational restructuring. For example, VA leadership granted the CIO authority over all IT funds in 2006. In addition, Congress approved legislation mandating the VA CIO to manage all IT resources and authorized a separate IT appropriation account for the VA in 2006.[22] Prior to this, the VA CIO had direct control over only 3 percent of the VA's IT budget and 6 percent of its IT personnel. Efforts to consolidate all IT planning and budgeting activities as well as restructuring IT personnel have provided the CIO with full control over the agency's IT investments. As a result, according to VA senior officials, the CIO is more effective in stopping funding for programs. For example, the CIO halted 45 underperforming IT programs in July 2009 and eventually canceled 12 of them. The CIO credits this type of success to having sufficient control over the IT budget.

The OCIO Plans To Improve Budget Planning

To help address these concerns, the OCIO plans to further its enterprise portfolio governance approach to ensure that component IT budget planning activities are more cohesive and strategic. As this is accomplished, budget planning should be conducted from a

[22] Section 222 of P.L. No. 109-114; H. R. Rep. No. 109-305, at 50 (2005) (Conf. Rep.).

portfolio perspective. Once in place, portfolio steering committees would analyze and consolidate capabilities, which would feed into the budget planning recommendations and result in budget requests that align with portfolio and departmental goals. The process is designed so that portfolio and program reviews are conducted prior to OMB and Investment Review Board reviews, thus resulting in decisions that can be factored into budget plans. The CIO expects that this approach, depicted in figure 10, will result in component-level IT funding plans that align with a unified portfolio and departmental strategy.

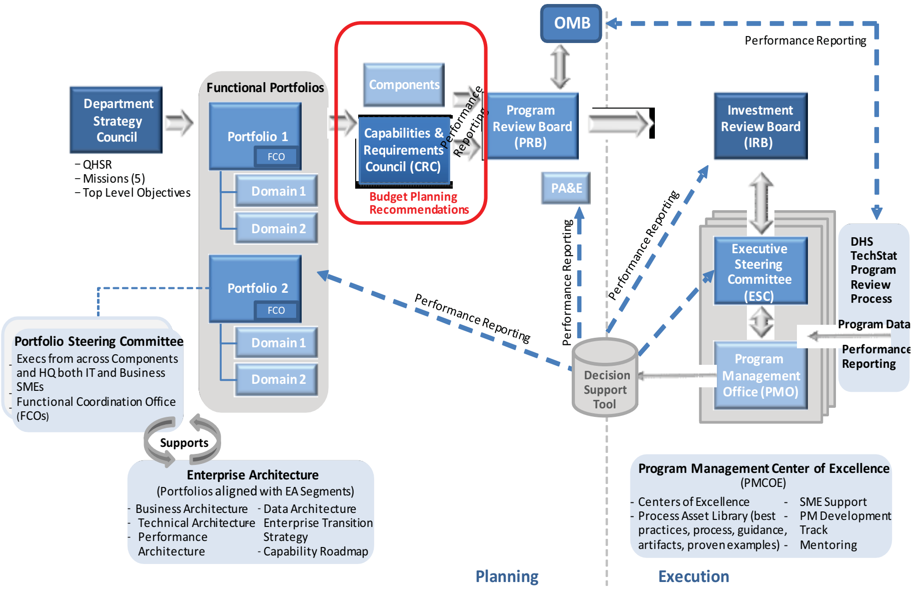

Department Strategy Council
– QHSR
– Missions (5)
– Top Level Objectives
Functional Portfolios
Portfolio 1
FCO
Domain 1
Domain 2
Portfolio 2
FCO
Domain 1
Domain 2
Portfolio Steering Committee
Execs from across Components and HQ both IT and Business SMEs
Functional Coordination Office (FCOs)
Supports
Enterprise Architecture
(Portfolios aligned with EA Segments)
- Business Architecture
- Technical Architecture
- Performance Architecture
- Data Architecture
Enterprise Transition Strategy
- Capability Roadmap
Components
Capabilities & Requirements Council (CRC)
Performance Reporting
Budget Planning Recommendations
OMB
Program Review Board (PRB)
PA&E
Performance Reporting
Performance Reporting
Performance Reporting
Performance Reporting
Decision Support Tool
Investment Review Board (IRB)
Executive Steering Committee (ESC)
Program Management Office (PMO)
DHS TechStat Program Review Process
Program Data
Performance Reporting
Program Management Center of Excellence
(PMCOE)
- Centers of Excellence
- Process Asset Library (best practices, process, guidance, artifacts, proven examples)
- SME Support
- PM Development Track
- Mentoring
Planning
Execution

Figure 10: Budget Alignment in DHS Governance Operating Model, Draft

This process, once fully implemented, should enable the DHS CIO to evaluate IT resource allocation plans from a portfolio perspective to promote effective alignment of IT resources. The DHS OCIO plans to mature its portfolio management approach to augment budget reviews and align IT investments with portfolios earlier in the budget cycle. However, until the OCIO fully implements its portfolio management approach, the CIO will be unable to ensure that IT acquisitions align with the Department's strategic goals and objectives.

Recommendation

We recommend that the Deputy Under Secretary for Management:

Recommendation: Assign the DHS CIO centralized control over the Department's IT budget planning process to review, guide, and approve IT investments.

Management Comments and OIG Analysis

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

In the comments, the DHS Deputy Under Secretary for Management concurred with our report recommendation and provided comments on specific areas within the report. We have reviewed management's comments and provide an evaluation below.

In response to our recommendation, the DHS Deputy Under Secretary for Management states that, consistent with the *Clinger-Cohen Act of 1996*, the OCIO is firmly integrated with the processes for making budget, financial, and program management decisions within the agency.

We do not agree that the OCIO is, as yet, "firmly integrated" into DHS IT budget processes. We determined that the CIO needs to participate earlier in the budget planning process so that the CIO can ensure that component IT budget plans are in alignment with departmental goals and objectives. As such, we look forward to hearing more about the Department's plans to ensure the CIO's integration into the Department's budget planning process to review, guide, and approve IT investments.

Appendix A
Purpose, Scope, and Methodology

As part of our ongoing responsibilities to assess the efficiency, effectiveness, and economy of departmental programs and operations, we conducted this audit to determine progress made in establishing CIO oversight and authority, achieving IT integration, improving IT management functions, and addressing our prior report recommendations.

We researched and reviewed Federal laws and executive guidance related to IT management and CIO governance. We obtained published reports, documents, and news articles regarding DHS CIO operations and IT management throughout the Department. Additionally, we reviewed recent Government Accountability Office (GAO) and DHS OIG reports to identify prior findings and recommendations. We used this information to establish a data collection approach that consisted of focused interviews and documentation analysis to accomplish our audit objectives.

We held interviews at DHS CIO headquarters and offices. We interviewed more than 20 DHS CIO headquarters officials, including the CIO, the Deputy CIO, executive directors, and branch leads to discuss their roles and responsibilities, progress in establishing CIO authority, improvements to management functions, and accomplishments toward achieving IT integration. We discussed CIO budget authority, IT portfolio management, and enterprise-wide IT services. We also met with the Program Accountability Risk Management within the Office of the Chief Procurement Officer to understand the enterprise acquisition process and the level of authority the Department's CIO has over IT acquisitions. We collected supporting documents about DHS IT management, the IT budget process, and current integration efforts. Further, we met with CIOs and Deputy CIOs at DOE, DOJ, HHS, USDA, and VA to learn best practices and CIO authority at external agencies.

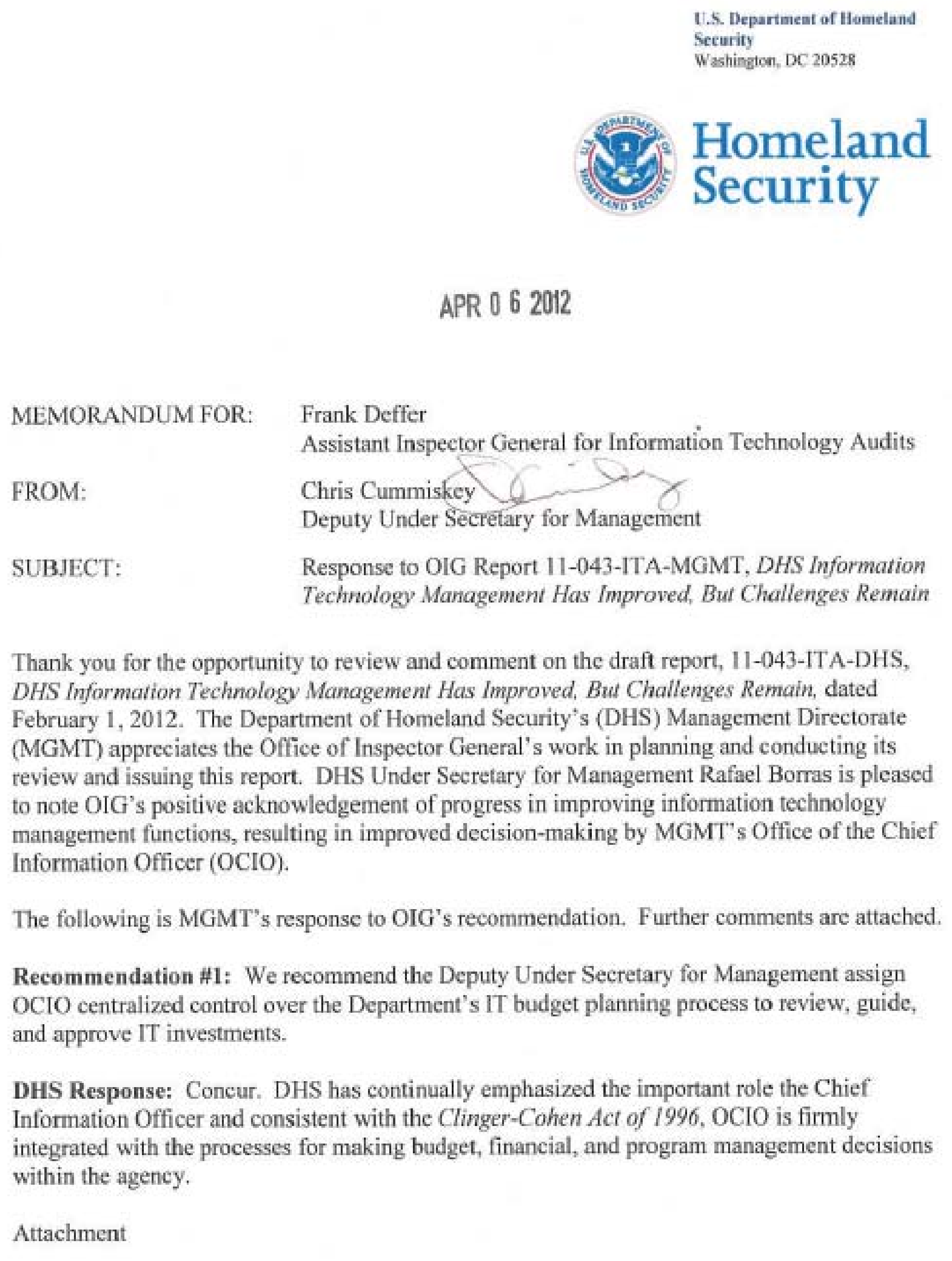
To assess the effectiveness of current departmental IT management practices, we interviewed CIOs and Deputy CIOs from the seven major operational components within DHS—CBP, FEMA, ICE, TSA, USCIS, USCG, and USSS—to discuss DHS IT management policies, DHS CIO budget authority, portfolio management, communication, and major integration efforts.

We conducted audit fieldwork from August to November 2011 at DHS CIO headquarters, operational component headquarters, and the headquarters of external agencies in Washington, DC. We conducted this performance audit pursuant to the *Inspector*

General Act of 1978, as amended, and according to 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions, based upon 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. Appendix D identifies major OIG contributors to the audit.

Appendix B
Management Comments to the Draft Report



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

Homeland Security

APR 0 6 2012

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Information Technology Audits

FROM: Chris Cummiskey
Deputy Under Secretary for Management

SUBJECT: Response to OIG Report 11-043-ITA-MGMT, *DHS Information Technology Management Has Improved, But Challenges Remain*

Thank you for the opportunity to review and comment on the draft report, 11-043-ITA-DHS, *DHS Information Technology Management Has Improved, But Challenges Remain,* dated February 1, 2012. The Department of Homeland Security's (DHS) Management Directorate (MGMT) appreciates the Office of Inspector General's work in planning and conducting its review and issuing this report. DHS Under Secretary for Management Rafael Borras is pleased to note OIG's positive acknowledgement of progress in improving information technology management functions, resulting in improved decision-making by MGMT's Office of the Chief Information Officer (OCIO).

The following is MGMT's response to OIG's recommendation. Further comments are attached.

Recommendation #1: We recommend the Deputy Under Secretary for Management assign OCIO centralized control over the Department's IT budget planning process to review, guide, and approve IT investments.

DHS Response: Concur. DHS has continually emphasized the important role the Chief Information Officer and consistent with the *Clinger-Cohen Act of 1996*, OCIO is firmly integrated with the processes for making budget, financial, and program management decisions within the agency.

Attachment

Appendix C
Major Contributors to this Report

Richard Harsche, Division Director
Kristen Bernard, Audit Manager
Craig Adelman, Auditor-in-Charge
Anna Hamlin, Auditor
Thea Calder, Auditor
Daniel McGrath, Auditor
Aaron Zappone, Referencer

Appendix D
Report Distribution

Department of Homeland Security

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

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, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, or e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

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

- Call our Hotline at 1-800-323-8603

- Fax the complaint directly to us at (202)254-4292

- E-mail us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:

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

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