DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

IMPROVEMENTS NEEDED TO DHS' INFORMATION TECHNOLOGY MANAGEMENT STRUCTURE

Office of Information Technology

OIG-04-30

July 2004

Office of Inspector General

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

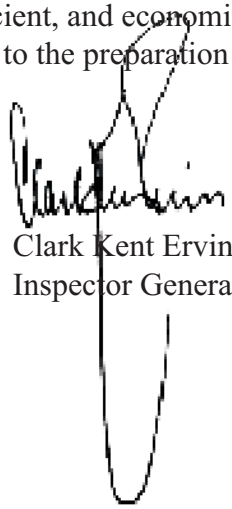
Homeland Security

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, investigative, and special reports prepared by the OIG as part of its DHS oversight responsibility to identify and prevent fraud, waste, abuse, and mismanagement.

This report assesses the strengths and weaknesses of the program or operation under review. 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 the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that this report will result in more effective, efficient, and economical operations. I express my appreciation to all of those who contributed to the preparation of this report.



Clark Kent Ervin
Inspector General

Contents

Appendices

Abbreviations

ACE	Automated Commercial Environment
CIO	Chief Information Officer
DHS	Department of Homeland Security
EAB	Enterprise Architecture Board
eMerge^2	Electronically Managing Enterprise Resources for Government Effectiveness & Efficiency
Energy	Department of Energy
FDIC	Federal Deposit Insurance Corporation

Contents

FISMA	Federal Information Security Management Act
IRB	Investment Review Board
IRP	investment review process
IT	information technology
OIG	Office of Inspector General
US-VISIT	U.S. Visitor and Immigrant Status Immigrant Status Indicator Technology
VA	Veterans Administration

Figures

Tables

Introduction

In today's environment, the effective management of information technology (IT) is not only critical to federal agency success, it is required by law. The Clinger-Cohen Act of 1996,[1] one in a series of key IT laws and executive guidance, requires that federal departments and agencies establish chief information officers (CIOs) to institute, guide, and oversee frameworks for managing IT systems and initiatives as strategic investments. Newly established in March 2003, DHS faces the combined challenge of positioning a CIO to comply with federal IT guidelines and bring the department together technologically to accomplish mission objectives and meet performance goals.

Results in Brief

The DHS CIO has a significant role to play in guiding IT resources and capabilities to fulfill the department's diverse missions. The enormous task of creating one network and one infrastructure to ensure IT connectivity among the department's 22 legacy organizations is daunting. In this context, some of the CIO's challenges are to implement an enterprise architecture; standardize and integrate the department's many duplicative systems and tools; and institute a program to address the risks and vulnerabilities facing DHS' IT systems.

Despite these key responsibilities, the CIO is not a member of the senior management team with authority to strategically manage department-wide technology assets and programs. There is no formal reporting relationship between the DHS CIO and the CIOs of major component organizations, which hinders department-wide support for his central IT direction. Further, the CIO has limited staff resources to assist in carrying out the planning, policy formation, and other IT management activities needed to support departmental units. These deficiencies in the IT organizational structure are exemplified by the CIO's lack of oversight and control of all DHS' IT investment decision-making. Instead,

[1] Also known as the Information Technology Management Reform Act, Div E, P.L 104-106

there is a reliance on cooperation and coordination within DHS' CIO Council[2] to accomplish department-wide IT integration and consolidation objectives.

The Department of Homeland Security would benefit from following the successful examples of other federal agencies in positioning their CIOs to meet federal guidelines. Specifically, repositioning the CIO to report to the Office of the Deputy Secretary would provide this official the authority and influence needed to guide executive decisions concerning department-wide IT investments and strategies. Having component-level CIOs report to both the DHS CIO and their respective agency heads would help ensure commitment to consolidating the IT infrastructure while also meeting business needs. Further, with adequate IT office support and control of all DHS IT investment decision-making processes, the CIO can better ensure successful accomplishment of IT objectives, programs, and initiatives.

Background

DHS relies on a variety of IT systems and technologies to support its wide-ranging missions, including counter terrorism, border security, and infrastructure protection. Advanced technologies and IT services are fundamental to support internal operations and to ensure the systems integration and information sharing needed to help protect the homeland in the wake of the September 11, 2001, attacks. DHS' IT budget in FY 2004 was about $4 billion–the third largest IT investment budget in the federal government–including operations and maintenance costs. Effective and strategic management is the key to maximizing the potential of these technology investments.

Taken together, a series of laws and related guidance provide a management framework for the new department to follow as it evolves and applies IT to meet its mission needs. The Paperwork Reduction Act of 1995,[3] designates senior information resources management positions in major departments and agencies with responsibility for applying technology to help reduce the government's information collection burden. The Clinger-Cohen Act of 1996 renames and elevates the former senior information resources manager positions to executive-level CIOs, who report directly to their agency heads and have IT

[2] The DHS CIO Council is comprised of the CIOs from each DHS component, ex officio representatives from General Counsel, the Chief Financial Officer's Council, the Office of the CIO, and the Executive Procurement Executive Council. The CIO Council was chartered to develop, promulgate, implement, and manage a vision and direction for information resources and telecommunications management within DHS.

[3] Public Law 104-13.

as a primary responsibility. Further, Office of Management and Budget Circular A-130–Appendix III–implements the Clinger-Cohen Act by establishing specific policies and procedures for effective IT management. Additionally, the strategies and practices of successful federal agencies provide useful examples and lessons learned that DHS may consider and apply in structuring itself to manage IT effectively.

FINDINGS

CIO Faces Major IT Management Challenges

The responsibilities of the DHS CIO, as set forth in the Homeland Security Act of 2002,[4] cover a variety of functions, including IT planning; budgeting and financial management; infrastructure management; systems development; IT human capital; and, support services such as the IT customer help desk. A deputy CIO helps provide enterprise-wide IT support in carrying out these functions. The deputy CIO is responsible for directing information management support processes, and combining IT and telecommunications to provide coordinated capabilities to meet DHS' information needs. The deputy CIO also is responsible for research, development, acquisition, and testing of new technologies to support DHS mission needs. In addition, the CIO has six acting directors who report to him in the following functional areas: applied technology, information security, infrastructure, information and application delivery, planning and enterprise architecture, and business support.

These officials, along with the CIO, face the highly complex challenge of managing IT in what constitutes the largest federal department reorganization in 50 years. Since the department's inception, the CIO has undertaken several initiatives to provide some degree of connectivity among the department's 22 legacy agencies, including linking e-mail systems and providing access to a shared online intranet portal. However, the larger tasks of identifying department-wide IT assets and creating a consolidated and secure IT infrastructure have yet to be accomplished. All are expected to achieve significant IT efficiencies and cost savings.

Creating a single infrastructure for effective communications and information from the disparate networks of its transferred agencies is the most important task facing DHS. To support this effort, the CIO has established an Enterprise

[4] Title VII, P.L. 107-296, as amended by P.L. 108-107.

Infrastructure Board that meets periodically to discuss strategies for connecting these local, metropolitan, and wide area networks. The Enterprise Infrastructure Board is comprised of project teams such as the Network Security Board, which is tasked with implementing an initiative to institute the firewalls, routers, switches, and other technologies needed to secure DHS networks. For example, DHS is enhancing the Immigration and Customs Enforcement's telecommunications "backbone" to create the department-wide network, which will establish data communications with common policies and technical standards among all of its organizational elements.

Further, the CIO has a key role to play in working with line managers to design and manage an enterprise architecture to guide management of information and technology in the department to help accomplish its many diverse missions. The CIO released the first version of the DHS enterprise architecture in September 2003, and is now working to align its transition strategy with several large projects in the department such as the Automated Commercial Environment (ACE) and the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT). Work is currently underway to complete a second version of the enterprise architecture and make the transition strategy more detailed and easier to implement.

Another challenge to the CIO is to consolidate the disparate networks, data centers, and systems of the legacy agencies. For example, over 100 redundant and nonintegrated systems are used to support a variety of administrative activities such as accounting, acquisition, budgeting, and procurement. Because of the lack of standardization and interoperability in the current environment, many of these activities are tedious and burdensome. To integrate these systems, DHS has established the "eMerge^{2}" program,[5] scheduled for implementation by September 2006. Further, DHS has responsibility for implementing at least 8 of the top 25 IT projects of civilian federal agencies. Along with eMerge^{2}, these projects include ACE, US-VISIT, the Integrated Wireless Network, and the Rescue 21 maritime communications system. The CIO has a major role to play in helping ensure that these systems are acquired and implemented to meet expectations of the component sponsors.

Additionally, to meet requirements of the Federal Information Security Management Act (FISMA), the CIO is charged with implementing an information security management program that addresses the risks and vulnerabilities facing

[5] Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency.

DHS' IT systems. As part of its 2003 FISMA evaluation,[6] the OIG reported that none of the DHS components had fully functioning IT security programs; and, there were a number of key areas including systems security risk assessment, planning, testing, and certification and accreditation that required management attention. The OIG recommended that the CIO designate information security a material weakness at DHS. Presently, the CIO is refining and updating IT security plans, policies, and procedures and has implemented an automated software tool to conduct self-assessments to better manage systems security.

CIO Organizational Structure Is Not Optimal

Despite federal laws and guidance on establishing effective IT organizations, the DHS CIO is not well positioned to meet the department's IT challenges. With limited resources to carry out his responsibilities, the CIO lacks the authority and the relationships with DHS executive, line, and IT managers across department components to guide them in applying technology to accomplish the department's missions. While the decisions on structuring and staffing the CIO organization were well intentioned, they have not provided the CIO a sound basis from which to pursue the goals of "one network, one infrastructure, one DHS." At this critical juncture in the department's evolution, the CIO would benefit from a more centralized IT management structure and additional staff support to help govern shared IT programs and services as well as to help better direct the components' mission and supporting technologies in a concerted manner.

CIO is Not Well Positioned to Guide IT Department-wide

Federal laws and regulations recognize the importance of IT to agency missions and emphasize the need for a centrally positioned, senior level proponent who is responsible for strategically managing technology assets and programs across the agency. Accordingly, federal guidelines require that each executive agency position a CIO as a member of the senior executive team with the accountability and responsibility to manage IT across organizational units. The CIO should report to the agency head, providing advice and assistance to this official on how best to implement and manage IT to improve productivity, efficiency, and effectiveness. Additionally, the CIO is to serve as a bridge between senior executives, line managers, and technical professionals to ensure that IT strategies

[6] *Information Technology: DHS Information Security Program Evaluation, FY2003*, Office of Information Technology, Office of Inspector General, Department of Homeland Security, OIG-IT-03-02, September 2003.

are communicated effectively and implemented department-wide. Where more than one CIO or senior IT official is designated, the respective duties of the officials must be clearly delineated.

DHS CIO is Not a Member of the Senior Management Team

The DHS CIO is not positioned effectively within the department's hierarchy to meet these requirements. The CIO, who does not report to the Secretary or the Deputy Secretary, is not a member of the department's senior executive management team. He does not serve as a peer to the DHS Under Secretaries or component directors, nor does he have the opportunity to discuss department-wide IT issues, such as IT planning, investment management, or budgeting, or have the power and influence to guide IT initiatives within DHS components.

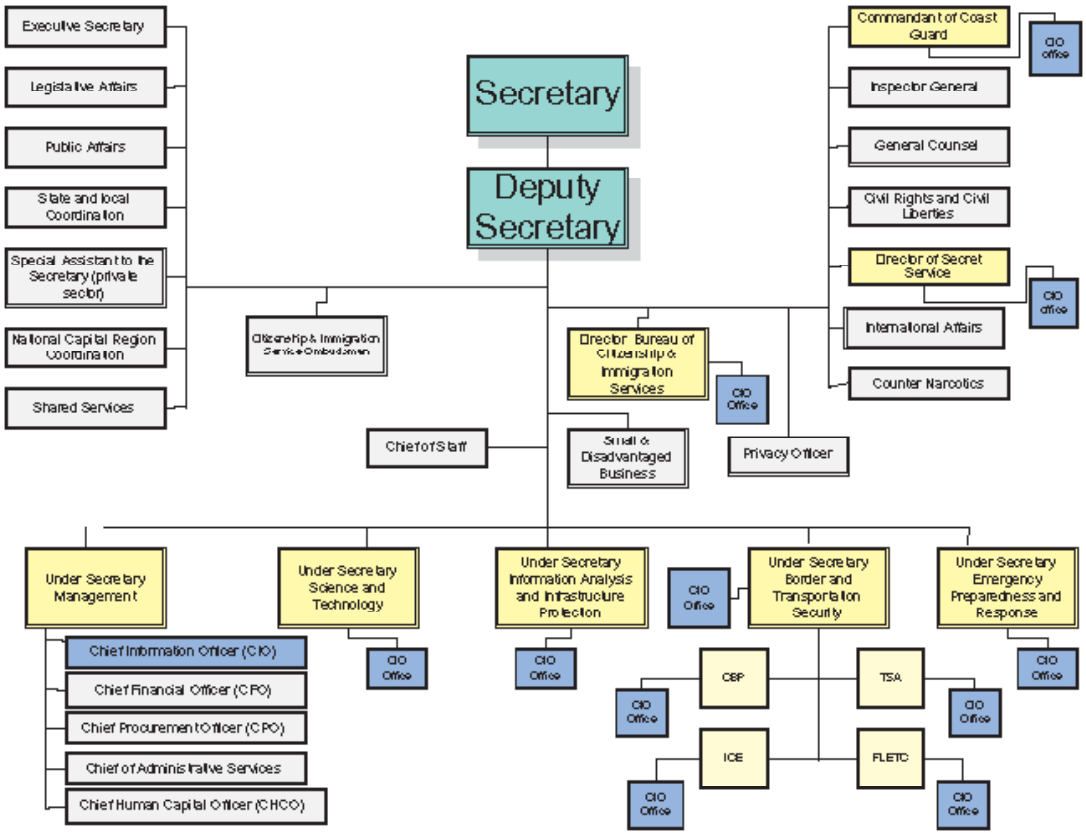
Rather, the CIO reports to the Under Secretary for Management, one of the department's major components. The CIO is a peer to other operational officers–such as the chief financial officer, the chief human capital officer, and the chief procurement officer–and competes with these officials for resources to carry out his specific responsibilities. Together, these officials meet with the Under Secretary on a bi-weekly basis to discuss and coordinate activities within their respective offices. In this forum, they can elevate unresolved issues among their various offices to senior management attention. They can also learn second hand about issues discussed at more senior executive levels within the department and their role in helping to accomplish department-wide program goals. Because there is no forum to routinely and directly raise IT issues with the DHS Secretary, the DHS CIO must appeal through the Under Secretary for Management for support. Also, the activities and budgets of the CIO are subject to approval by the Under Secretary for Management.

At this subordinate level, the CIO has no authority over the more senior component directors that he is supposed to be overseeing in terms of IT. The CIO must rely on informal channels, rather than the official reporting structure, to accomplish IT objectives. For example, according to DHS IT officials, the CIO leverages his working relationships with former IT staff who have transferred to various directorates to promote IT shared services objectives and build working relationships with component line managers.

Component CIOs Not Linked to DHS CIO

There is no documented, formal reporting relationship between the DHS CIO and the CIOs of the major DHS component organizations. Officially, these CIOs report to their directorate managers–but not to the DHS CIO. As such, the DHS CIO does not have the power or influence to guide IT initiatives across the department. Figure 1 provides a DHS organization chart depicting these CIO relationships.

Figure 1: DHS Organization Structure



There is no written policy to indicate the DHS CIO's role towards the component CIOs or their IT infrastructures. Policies to define and communicate these roles and responsibilities of the component level CIOs and their technical staff vis-à-vis the DHS CIO do not exist. For example, the majority of DHS network administrators do not report through a chain of command that links to the DHS CIO. Although the DHS CIO is responsible for management of the IT

infrastructure, he does not have any administrative or technical control over the components' disparate networks.

Further, in some instances, the directorates do not involve or apprise the DHS CIO of their individual IT projects or initiatives. Component IT managers and their staff might be required to support their respective directorates on initiatives that may directly contradict or interfere with initiatives of the DHS CIO. For example, leadership in some directorates is resistant to the idea of transferring any of their IT infrastructure to the control of the CIO, with the belief that, if anything were to go wrong in support of their missions, they, not the DHS CIO, would be held accountable. Department-wide support and buy-in will be critical if the CIO is to achieve the objective of "one network, one infrastructure" by December 2005.

CIO Staff Resources Are Inadequate

Despite his wide-ranging responsibilities for consolidating DHS' IT infrastructure, the CIO has a small staff consisting of IT and systems security specialists and IT policy, planning, management, and budget analysts, to support him. Across the six functional areas, the CIO only has been authorized to hire about 65 employees to support a department of over 180,000 employees. As of May 2004, only 49 of these positions were filled. Officials throughout the department have expressed concern that this is an inadequate number of staff to meet the many challenges in providing IT support services and consolidating technology systems, facilities, and initiatives across 22 different components in the new department.

The CIO has relied upon detailees from other component organizations as well as contractors to help satisfy the large amount of work that remains to be accomplished. For example, two of the directors in the office of the CIO are on loan from other organizations. Further, a CIO working group formed to develop the first version of the DHS enterprise architecture consisted of detailees from various DHS organizational elements. According to the director of Planning and Enterprise Architecture, understaffing and inadequate support from the CIO office resulted in the detailees working overtime each day for several weeks to meet the August 1st deadline for developing the enterprise architecture. In May 2004, the CIO estimated that his office had about 121 contractors and detailees on staff.

The benefit to having the detailees and contractors on board is that these personnel can become familiar with the organization and its systems and can share best practices to help foster improvements. In some instances, it is easier to find

subject matter experts within the ranks of detailees and contractors on fairly short notice than to wait for full-time hires. In other instances, the temporary employees may lack the expertise needed to be effective. Another problem is that there is a loss of continuity of services when the detailees or contractors return to their home offices or are reassigned.

In comparison with the DHS CIO resources, the individual components within the department have much larger IT staffs, which they brought with them when they became part of DHS in 2003. Few, if any, are under the purview of the DHS CIO. Some of the individual component IT shops within DHS are proportionately much bigger than the DHS CIO's office. For example, as the Government Accountability Office (formerly the General Accounting Office) reported in May 2004,[7] the CIO organization of the former Federal Emergency Management Agency[8] has about 262 permanent employees and approximately 70 temporary (disaster-related) employees. The Transportation Security Administration reports that its CIO organization has roughly 145 employees. The Coast Guard reports that its CIO organization has approximately 140 employees. Together, these three component CIO organizations account for about 600 positions and control about $3.6 billion in fiscal year 2004 IT budget and spending.

CIO officials told the OIG that given their relatively small staff resources they have been "busy putting out fires" in efforts to help get the new department up and running. As a result, they have been hindered in carrying out some of their critical IT management responsibilities. For example, they have not been able to put in place all of the plans to govern IT human capital management across the department. Likewise, they have not been able to institute the central guidance and standards needed for functions such as information security, network management, telecommunications, or web-based applications. Further, the CIO office has not had the chance to institute a systems development life cycle methodology or update established IT policies and procedures. Without such up-to-date, documented IT direction, inconsistencies in the department-wide processing environment could occur.

To maximize the potential of its limited staff resources and ensure productivity, the CIO uses a matrixed management approach to accomplish IT responsibilities. This means using a variety of support staff, project teams, and working groups. Each of the five directors in the CIO office has a working group with cross-agency

[7] *Information Technology: Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems*, U.S. General Accounting Office (GAO-04-509, May 21, 2004).

[8] The former Federal Emergency Management Agency now comprises the Emergency Preparedness and Response directorate within DHS.

representation to support efforts in their functional areas regarding enterprise-wide programs. The benefit of the matrixed management organization is that it integrates various viewpoints, resulting in more cross-agency and thorough decision-making.

One of the component CIOs said that the matrixed approach is patterned after a model designed by the former CIO of General Motors Corporation in the late 1990s. At General Motors, information officers were responsible for educating the senior management teams on the value of IT, while process information officers were responsible for identifying common processes and systems across business units. Both positions reported directly to the corporate CIO, as well as their respective unit executives. This matrixed staffing model helped ensure accountability in the large, complex General Motors organization. However, the model is not readily applicable to DHS because, whereas the General Motors CIO was part of the senior executive team and had significant authority over IT as well as the business, the DHS CIO is positioned at a lower organizational level and does not drive IT department-wide. As one industry CIO observed, an IT manager needs business clout–not a "stick," but power and influence through top leadership buy-in to ensure the ability to accomplish business change.

DHS Had Discretion in Establishing its IT Organization

The current IT management structure can be traced back to the Homeland Security Act, which authorizes the DHS Secretary to position the CIO discretionally within the organization. DHS managers told the OIG that officials within the White House Office of Homeland Security made the decision to have the CIO report to the Under Secretary for Management. The Under Secretary for Management was in agreement with this reporting relationship.

The limited CIO office staffing dates back to the inception of DHS and is, according to senior DHS officials, the result of a cap set on overhead expenses and staff resources for DHS headquarters. The Management Directorate, as well as the Secretary's office, was limited to a total of 800 employees. Of the 800, a total of about 65 staff was allotted to the CIO office.

Another contributing factor to the problems with limited staff resources is that all employees in the CIO office must have at least secret level clearances. Obtaining a clearance is a time-consuming process managed by the Office of Personnel Management and largely beyond DHS control. According to the chief human capital officer, because of the Office of Personnel Management's backlog of new

recruits requiring background investigations, it currently takes an average of about 250 days to hire an employee.

DHS CIO Would Benefit from Greater Organizational Authority and Staff Resources

While there is no one way to position a CIO, the best approach is to structure the IT organization to meet the existing need. In our opinion, the decentralized IT model that DHS has chosen is not the appropriate one at this critical time as the department evolves, integrates, and institutionalizes its operations. Senior IT experts said that IT decentralization may be effective in well established organizations with well defined authorities, management reporting relationships, and accountabilities. Senior IT officials also indicated that IT decentralization might work in entities that are smaller and relatively easy to control.

However, decentralized IT is not effective in a large, complex organization like DHS, which is still working to eliminate duplication, integrate systems, and achieve IT sharing and unity across its 22 legacy agencies. More centralized CIO control is particularly critical at DHS where component missions and objectives are often in conflict with one another. A central advocate may be needed to decide amongst them. For example, both the US Citizenship and Immigration Services and the Customs and Border Protection directorates are developing case management systems. The DHS CIO initially opposed acquiring two separate systems with essentially the same functionality, viewing the duplication as a wasteful investment. However, the director of the U.S. Citizenship and Immigration Service overrode the CIO's intention to make this a shared endeavor.

CIO Does Not Manage IT Department-wide

The deficiencies in CIO positioning and authority are exemplified by the fragmented manner in which IT investments are managed across the department. Although federal guidance calls for CIOs to play a key role in managing department-wide IT resources, the DHS CIO has a limited role in the department's investment review process. It is largely confined to consensus building to manage infrastructure and selected joint or consolidated systems while mission applications and component level IT investments continue to be managed in a decentralized manner. Such oversight limitations hamper CIO progress in

accomplishing the vision of eliminating redundancies among the legacy IT systems and programs at all levels across the department.

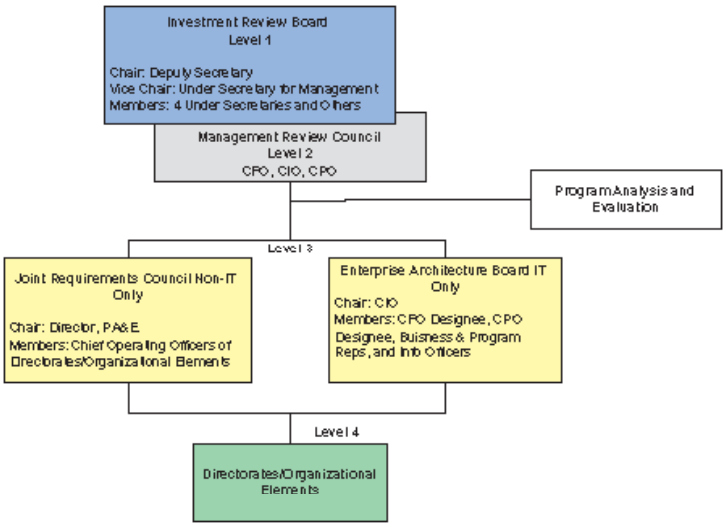
CIO Does Not Oversee All IT Investments

Federal guidelines give the CIO, in partnership with senior agency executives, the responsibility for ensuring effective management of organization-wide IT to support agency business and missions. To help carry out this responsibility, CIOs are to play a key role in disciplined agency investment review processes for selecting, controlling, and evaluating IT investments to help maximize return on investment and accomplish mission objectives and results.

According to these requirements, DHS has taken steps to establish a process for its investment decision-making and management. Specifically, *Management Directive Policy #1400: Investment Review Process* provides guidance for reviewing both IT and non-IT investments in the department. DHS' investments are categorized into four levels based on a combination of factors, including mission criticality, dollar thresholds, and sponsorship. The levels specify the documentation required for the IT investment review, as well as what office or official within the department's hierarchy is responsible for making the investment approval and oversight decisions.

However, the CIO does not oversee or control the process for managing IT investments at all levels throughout the department. The following figure provides an overview of the DHS investment review process (IRP) and is followed by a discussion of the CIO's role at each investment level.

Figure 2: Overview of DHS' Investment Review Process



Major and Mission Critical Investments

The CIO is not the principal proponent for Level 1 investments, which are mission critical programs with contract costs over $50 million. Rather, a DHS Investment Review Board (IRB) headed by the Deputy Secretary is responsible for reviewing major, mission-critical investments–both non-IT and IT–at this level. The projects are reviewed for approval and progress, primarily based on "Exhibit 300"[9] business case documentation, which is developed for submission to the Office of Management and Budget pursuant to the annual budget process.

The IRB consists primarily of DHS senior executives from each DHS major component, along with other key officials from the office of the Under Secretary for Management. The CIO is a voting member of the IRB and, as needed, may be called upon to provide guidance on IT investments to more senior level officials. However, the CIO does not have the final say in "Level 1" IT decisions. For example, officials told the OIG that although the CIO did not recommend continuing with development of a second case management system within Customs and Border Protection, the Deputy Secretary decided to proceed anyway. The CIO's rationale was that a comparable case management system already under development in CIS could provide the functionality needed for both components.

[9] Exhibit 300s are documents by which project teams can demonstrate to agency management and the Office of Management and Budget that they have employed the disciplines of good project management, represented a strong business case, and met other federal requirements to define the proposed cost, schedule, and performance goals for an investment if funding approval is obtained.

Further, because the CIO does not manage the investment process at "Level 1," he cannot ensure that major IT investment reviews are conducted in a timely manner to provide the approvals necessary at key points during a system's life cycle. Financial officers are responsible for coordinating meetings of the IRB. Despite the amount of money expended on major IT systems and initiatives across the department, the IRB has held infrequent meetings to oversee these investments. Many of the meetings scheduled have been cancelled or postponed.

Specifically, since May 2003, the IRB has scheduled 21 meetings, but postponed or canceled 12 of them. Several were related to highly visible IT initiatives such as US-VISIT, IT infrastructure, and the SAFECOM project for wireless communications to support emergency response. Senior DHS officials said the IRB delays are due to its high-level membership with competing priorities and the fact that the board is just starting out and as yet has no sense of urgency to get things done. Financial officers attributed the missed meetings to inadequate business case information provided by the responsible units to support their programs. These officials said that it is a major challenge to get DHS components to adequately prepare this information in advance for the IRB reviews. Similarly, in its feedback on the President's budget for FY 2005, the Office of Management and Budget stated that while over half of DHS' business cases were acceptable, continued improvement is still needed.

Missed milestones due to the IRB meeting cancellations have placed some projects at risk. For example, Customs and Border Protection officials told the OIG that an August 2003 IRB review of the Automated Commercial Environment project was repeatedly rescheduled to the point where some parts of the project ran out of funding and the project was placed on hold. The project did not get the funding it needed to see it through the remainder of the fiscal year until the IRB met and reviewed the project in December 2003.

Significant "Level 2" Investments

The Management Review Council, responsible for "Level 2," has never met. This Level is comprised of significant IT initiatives with contract costs from $5 to $50 million. The Management Review Council is to review high visibility IT and non-IT programs that may impact more than one DHS component. These reviews are to be based on "Exhibit 300" budget documentation or a subset thereof. According to *Management Directive #1400*, the Council is comprised of the CIO, the Chief Financial Officer and the Chief Procurement Officer. However,

approval and decision-making authority regarding Level 2 programs rests with the directorate heads and under secretaries for the program's sponsoring directorate.

Component-level IT Investments

Just as there is no formal reporting relationship between the DHS CIO and the component level CIOs, the DHS CIO also does not control "Level 4" investments. This level is comprised of IT investments for directorates or organizational elements that cost less than $5 million. Rather, senior officials in the DHS components have approval authority for these systems investments. The costs for component systems are generally included on the "Exhibit 53" IT budget summaries annually submitted to the Office of Management and Budget.[10] A number of DHS components also have their own processes for reviewing and managing their IT investments apart from DHS CIO purview. Although the CIO is supposed to review and approve the component's investment management processes and randomly select "Level 4" investments to ensure compliance with IT review procedures, this is not being done.

The DHS CIO may not be aware of all IT systems that are being implemented by components in DHS. DHS field offices have implemented systems that do not comply with CIO standards and requirements. For example, without the DHS CIO's knowledge, one office had implemented a mission critical web-based application without the appropriate investment planning, documentation, and cost estimates. While financial management officials said that such systems are accounted for in the department's "Exhibit 53" IT investment portfolio submitted to the Office of Management and Budget, only major programs are line items in this document and the system was not included. The application has not been certified and accredited, although sensitive information on people is stored in the system. A DHS field office created the application using open source code in a program that is not supported by the component CIO. At one time, the system even used a ".com" web address rather than the required ".gov" web address.

This system is not currently on the department's network. However, given field office independence, the component CIO believed that this could certainly be done without his or the DHS CIO's knowledge, posing significant security vulnerabilities. Other organizational elements could independently be purchasing systems that may not work together with the overall DHS technical foundation

[10] An exhibit 53s is a roll-up of an agency's major IT programs to comprise the agency's IT investment portfolio. This report, submitted to the Office of Management and Budget as part of the federal budget process, provides the basic information that an agency needs to link its planning, budgeting, acquisition, and management of IT resources.

and thus not meet DHS mission and business needs or performance objectives. Greater central CIO oversight and control would ensure more discipline in department-wide IT investment management practices.

Joint, Consolidated, or Cross-Cutting IT Investments

It is at "Level 3" that the CIO has the most responsibility over IT investments. "Level 3" programs have annual costs of $1 to $5 million or life cycle costs of $5 to $20 million. At this level, the CIO chairs an Enterprise Architecture Board (EAB), which is essentially the same body as the CIO Council, transformed to constitute the EAB when an investment decision must be made. The EAB is comprised of component-level CIOs and chief financial officer and chief procurement officer designees. According to *Management Directive #1400*, the EAB should include crosscutting business line managers; however, these officials only attend meetings on an as needed basis. Rather, the EAB generally includes only IT personnel and, as such, does not provide a venue for including business perspectives on IT directions.

Management Directive #1400 does not explain the EAB's role or its transformation from the CIO Council. Because there are no minutes from EAB meetings, the OIG was unable to verify EAB proceedings or results. However, *Management Directive #1400* states that the board supports department-wide strategic planning and helps establish strategic guidance. The EAB also reviews and approves individual IT system investments, such as US-VISIT. The CIO uses the board to identify joint or consolidated IT programs that can help integrate and create efficiencies across the department.

The board is responsible for reviewing programs to ensure alignment with the department's enterprise architecture. Version one of architecture, was released in September 2003. In addition, in the context of the EAB, the CIO in conjunction with the chief financial officer established the "eMerge^{2}" program as an enterprise architecture pilot program. The objectives of the program are to transform DHS business and financial policies, processes, and applications and eliminate disparate, redundant, and non-integrated systems. The requirements and architecture development contracts for the "eMerge^{2}" program were awarded in December 2003. The CIO's director of Planning and Enterprise Architecture has been assigned as the contracting officer representative and is responsible for administering and monitoring the "eMerge^{2}" program to ensure compliance with the contract terms and conditions.

Although the CIO is responsible for implementing improvements throughout the department's IT infrastructure, the CIO actually owns relatively little of these resources. The CIO basically controls the DHS headquarters infrastructure, which includes the backbone and some of the crosscutting IT programs and services. For example, the CIO controls the routers, switches, and hubs comprising the department-wide network. His office outlines the policies and guidance related to IT infrastructure products and services, and provides operational support to DHS headquarters elements in this regard. The office also administers the department-wide security program, providing the tools and support to safeguard and report on security of IT assets in line with FISMA requirements. Further, his office is responsible for web portal capability and delivery of information through the DHS Intranet and Internet sites. The CIO does not own any of the many mission and administrative systems and facilities within the various components, such as mission-specific applications and data centers. The IT infrastructure managed by the CIO amounts to only $185 million of the department's total $4 billion budget for information technology.

CIO Relies on CIO Council Forum to Accomplish IT Objectives

Given that the CIO does not control much of the department's IT programs, he relies on communication, cooperation, and coordination in the context of the CIO Council to work towards achieving the objectives of a unified DHS IT infrastructure. The CIO Council is comprised of the CIOs from each DHS component, ex officio representatives from General Counsel, the Chief Financial Officer's Council, the Office of the CIO, and the Executive Procurement Executive Council. The CIO Council was chartered to develop, promulgate, implement, and manage a vision and direction for information resources and telecommunications management within DHS. The council is a forum for discussing and coordinating IT systems and programs that are new or have potential for DHS-wide impact. Council members also advise the CIO on policy and fiscal issues having a direct bearing on IT and the abilities of the components to perform their individual and collective missions. The CIO uses the Council as a means to gain cooperation among DHS components regarding opportunities for IT consolidation, common infrastructure services, and information sharing with other agencies. Such cooperation is especially critical when component leadership initially may not want to give up resources to support department-wide IT initiatives.

However, rather than an authoritative and strategic decision-making body, the CIO Council has evolved into a large information-reporting session where the

individual CIOs share updates about the IT activities within their organizations. One IT official described the Council as a free flowing, unstructured body that lacks focus to move beyond talking about IT issues. This is reflected in CIO Council meeting minutes where "decision items" are really administrative action items for future meetings rather than productive outcomes. Further, once the decision items have been completed, there is little documentation of the outcomes or deliverables in subsequent meeting minutes.

The CIO Council is supported by a multitude of committees, working groups, and boards that were established in an ad hoc manner and often have unclear or overlapping functions, creating a confusing IT governance environment. For example, one IT manager indicated that each division within the CIO office has its own working group that meets periodically with people throughout the department to keep everyone abreast of new IT developments and opportunities for cross-functional solutions. Nonetheless, IT officials said that they plan to create still other working groups to address IT issues as they arise. Another IT official indicated that a Technical Review Board was created on paper, but has never held a meeting. Similarly, per CIO Council minutes, a Web Services Board has been has been awaiting a charter for over two months, but it has never come to fruition. The DHS CIO estimated that more than 40 different IT working groups have been established. However, his office could not provide the OIG with a complete list of the many different forums. In February 2004, the DHS CIO discussed plans to disband some of these working groups and consolidate the remainder into centers of excellence**.**

Opportunities Exist for CIO Management Structure Improvements

A number of government agencies successfully aligned their CIO management structure according to relevant IT legislation. These successful CIO organizations provide useful practices and lessons learned that DHS could adopt to help improve its IT management. Their practices might also be considered and applied as part of efforts underway to transition DHS to a more centralized IT support operation.

Examples of Effective Federal CIO Organizations

The OIG met with senior IT officials from three other agencies to discuss how, based on federal guidelines, they structured their IT organizations to effectively support mission needs. Specifically, the OIG visited the CIOs of the Veterans

Administration (VA), Federal Deposit Insurance Corporation (FDIC), and the Department of Energy (Energy), organizations that are either comparable to DHS in terms of complexity or were recommended by the DHS officials as models for potential review. The CIOs at these organizations told the OIG about the IT authority afforded them via organizational positioning and reporting relationships, supporting office structures, and control of IT investment review processes. The following table summarizes this information in comparison with the DHS CIO management structure.

Table 1: Comparison of DHS and Leading CIO Organizations

AGENCY	Reports to the Agency Head	CIO Controls Senior IT Managers Agency-wide	Total Agency Staff	IT Full-time Staff Under CIO Control	IT Contract Staff Under CIO Control	FY 04 $ Total IT Budget (Billion)	CIO Controls All IT Assets	CIO Controls IRP Process
DHS	No	No	180,000	49	121	4.0 B	No	No
Energy	Yes	Yes	14,500	113	207	2.7 B	Yes	Yes
FDIC	No	Yes	5,305	400	540	.219 B	Yes	Yes
VA	Yes	Yes	211,764	300	550	1.5 B	Yes	Yes

Unlike DHS, two of the three other federal CIOs report directly to their agency heads. While the CIO of the FDIC reports to the chief operating officer rather than the chairman, the CIO nonetheless attends the chairman's meetings and can directly advise and influence this official on agency-wide IT matters. Further, the other CIOs have authority over component IT managers and all IT assets within their organizations. This is not so at DHS. Additionally, IT staff under the DHS CIO's control are significantly fewer than at the other agencies. For example, the CIO at the VA, which is most comparable in size and budget to DHS, has 300 IT staff while the DHS CIO only has 49. The following case studies provide more details on the individual CIO organizations studied.

Energy CIO

The CIO at the Department of Energy reports directly to the Secretary and Deputy Secretary, with the ability to provide each with technical advice–a critical aspect of the CIO function. The CIO is also a member of the executive management team–a peer to the Under Secretaries, the Chief Financial Officer, and other senior program officials from component organizations. As such, the CIO has the authority and control needed to strategically manage IT across the department.

The CIO partners closely with the Chief Financial Officer on initiatives such as electronic government and is a member of key advisory boards and committees. Previously, the Energy CIO was positioned in different offices within the department's organizational structure, including the human resources, and management and budget offices. However, the incumbent believes that the CIO's current reporting relationships are highly effective and in line with Clinger-Cohen Act requirements as well as leading agency practices.

The Energy CIO has the resources and commitment needed to support the department's IT environment. Specifically, the Energy CIO has a deputy CIO, five associate CIOs, 113 full-time staff, and 207 contractors to support her. Collectively, they are providing IT support to the department's 14,500 employees. To ensure that department-wide needs are adequately represented, the Energy CIO works with associate CIOs from the various component organizations who serve as liaisons to their respective business and program units regarding major IT initiatives. These liaisons do not report directly to the CIO. However, because the Energy CIO is an equal partner with the Under Secretaries responsible for the components, the CIO can oversee and provide input and technical advice regarding component IT operations.

The Energy CIO has oversight of all IT investments and has instituted mechanisms to ensure the effective application of technology to help carry out the agency's missions and business. For example, the CIO developed an IT Strategic Plan aligned with the department's overarching strategic business plan. In addition, the CIO is responsible for creating all policies and procedures regarding IT issues. The Energy CIO also has developed an enterprise architecture and standards for guiding IT investments and modernization initiatives, and ensures that they support the agency plan. The architecture will be used to help break down some of the IT stove pipes that still exist in the organization. Currently, the CIO is conducting a study to inventory all IT assets to determine which can be consolidated and possibly contracted out.

The Energy CIO is a major player in the department's capital planning and investment control processes. In the context of these review processes, the CIO can ensure that department-wide IT investments are aligned with IT strategies, policies, and architectures and meet performance expectations. The CIO co-chairs a Technical Review Board that serves to guide and oversee IT investment initiatives throughout the department, which uses a balanced scorecard approach to measure IT performance. The CIO has instituted about 30 management directives to support IT planning and investment control processes. For Example,

investments are presented to a Capital Review Board–the ultimate investment decision-making body within the department, chaired by the Deputy Secretary. The review board is responsible for a range of strategic management and investment decisions regarding all types of programs, including IT. As a voting member of the Capital Review Board along with all other department executives, the CIO has been able to strategically align IT programs to support department-wide needs. Committed to IT success, the Secretary and the Deputy Secretary have also established a committee to monitor performance in areas such as cyber security and e-government to improve Energy's grade on the Office of Management and Budget's scorecard for IT.

FDIC CIO

The FDIC CIO does not report directly to the chairman for day-to-day matters, but reports to the Chief Operating Officer directly under the Chairman. Despite this reporting structure, the CIO's authority is not diminished because he has direct access to and meets routinely with executive-level decision makers. For example, the CIO attends all of the FDIC Chairman's senior staff meetings and has the opportunity to influence the chairman on agency-wide IT initiatives. In addition, the Chairman provides input to the CIO's performance appraisal and how CIO activities will be measured to gauge performance. As such, the CIO is considered a member of the senior executive team, actively participating in and helping to guide all IT investment decision-making.

The FDIC CIO's office is centrally organized, with three deputy CIOs heading an IT division of approximately 400 federal employees and up to 540 contractors. Collectively, they provide all IT support to the agency's approximately 5,300 employees, from IT planning to systems acquisition to help desk support for headquarters, including national infrastructure support. To manage the IT organization, the CIO office holds regular briefings with agency division directors to review program status and monitor progress. In addition, the CIO recently established and chairs an internal agency CIO Council that includes senior level business office executives, and serves as an advisory body to the CIO. The CIO Council meetings establish the agency IT plan and strategies, and ensure that business entities support IT decisions and that, in turn, IT is applied effectively to meet business needs.

The CIO also uses the CIO Council meetings to discuss and define IT planning strategies. Key outputs from the council consist of the IT strategic plan, which outlines IT goals and strategies as they align with the agency business goals

and mission. With the help of the CIO Council, the CIO is currently creating a strategic road map to ensure that all systems fit into the common infrastructure. The agency is updating its system development life cycle methodology, which will form part of a more consistent project management approach. Further, the CIO is responsible for developing all IT policies and procedures, using the CIO Council as a mechanism to solicit opinions and gain agency buy-in on these documents.

The CIO has oversight over all IT investment initiatives and has put in place reporting mechanisms for ensuring the effective application of technology to help carry out the agency's business mission. The CIO and Chief Financial Officer co-chair the corporation's capital review investment committee, which considers, approves and monitors all major agency capital projects. The committee reviews business cases and budgets for each IT initiative. For example, when funding or contracts are needed for a project, the request must be taken to the committee for approval. The capital investment review committee reports quarterly to the FDIC board of directors on how IT initiatives are performing, thus ensuring that milestones are met.

VA CIO

At VA, the CIO reports to the Secretary–a position which affords the officer the opportunity to provide IT technical and investment management advice at the most senior level within the department. The CIO is a member of the senior management team and a number of different boards and committees within the department as well, giving him the opportunity to build relationships and discuss IT initiatives with peers and line managers from three large VA components: the Veterans Benefit Administration, the Veterans Health Administration, and the National Cemetery Administration.

Previously, VA was a decentralized organization, but has since moved to a more IT centralized management structure that includes clear accountability and performance monitoring. Specifically, IT professionals in the field report to both the office of the CIO and their respective facility directors, making them accountable to both IT and the business for their work. While the CIO office develops the IT employees' performance appraisals, the facility directors provide input to these appraisals. Service level agreements and memoranda of understanding govern these reporting relationships. The new structure gives the CIO the authority and resources needed to manage IT systems and support operations at all hospitals and facilities across the VA.

The CIO is supported by three deputy CIOs, four division directors, and 7,000 technical specialists to assist in carrying out department-wide IT responsibilities. The CIO's IT budget is $1.5 billion per year, excluding another $1.5 billion allotted for research and development. CIO responsibilities include IT strategic planning, budgeting, investment management, policy and standard setting, network security, telecommunications management, and enterprise architecture development for the entire department. The CIO office spent 100 days deliberating with a working group of representatives from across the department to reach common ground and produce the first version of the architecture; they are currently developing the third version of the document.

The CIO heads an IT investment board which brings together senior managers from across the department to discuss IT initiatives and make investment decisions. IT investment decisions are subsequently submitted to a senior management council for review, and then on to the Deputy Secretary. The Deputy Secretary makes the final investment recommendations to the Secretary who is the ultimate decision-making authority. When investment decisions are time-critical, the VA CIO, as a member of the senior management team, has the option to go directly to the Secretary. The CIO said that this investment process is highly effective, as evidenced by the fact that for FY 2005, for the first time, the Office of Management and Budget approved all of the department's business cases for IT investments upon initial submission.

DHS Plans for IT Management Centralization

Currently, there are plans under consideration in DHS that, if implemented, could significantly affect IT and address many of the concerns raised in this report. Specifically, on September 12, 2003, the Secretary issued a memorandum to DHS senior leadership announcing his intention to consolidate and integrate DHS-wide support functions, including the Office of General Counsel, Human Capital Services, Administrative Services, Procurement Services, Budget and Finance Services, and Information Technology. To comply with the Secretary's memorandum, the Under Secretary for Management drafted a decision memorandum outlining possible solutions to consolidating all directorates under her purview. As part of the decision memorandum, the Under Secretary solicited information from each senior manager regarding ways to centralize their respective offices.

Together, the DHS CIO and the CIO Council have determined that centralization is necessary for the effective delivery of infrastructure and IT services. In

response to the Under Secretary's request for information, the CIO outlined a draft transition strategy, endorsed by the CIO Council, that serves as an attachment to the decision memorandum, discussing a service delivery model for all IT services customized to meet the mission needs of the DHS legacy agencies. The draft plan includes a timeline for all centralization functions to be completed within 100 days of initial implementation.

Under the transition plan, the DHS CIO would manage the IT infrastructure (i.e., local and wide area networks, telecommunications, applications server hosting, and collaboration services) and operations (help desk, network operations center, data centers, and continuity of operations). All support services personnel would be transferred to report directly to the DHS CIO. A CIO within Management would be responsible for enterprise applications related to human resources, financial, and administrative functions. Component CIOs would continue to manage mission applications and provide IT services and support for their respective component operations, with additional oversight by the DHS CIO to ensure that departmental IT goals and objectives are met. Mission support personnel would have a dual reporting relationship to both the DHS CIO and the mission leadership.

Furthermore, the Chief Information Security Officer would manage IT security policy and operations for the DHS CIO. Individuals and contracts responsible for supporting delivery of the IT infrastructure and security services would be reassigned to the respective DHS CIO office infrastructure and security organizations. In addition, the office of the CIO would have the authority to appoint business representatives to each component to ensure that mission requirements are well served by the new service delivery model.

The CIO Council plays a major part in the draft transition plan as well. The CIO Council–guided by the DHS enterprise architecture, the IRB, and federal laws such as the Clinger-Cohen Act and FISMA–would provide the decision authority for policy issues affecting the IT function. As chair of the CIO Council, the DHS CIO would have the final authority and responsibility for meeting IT missions and objectives. The CIO Council would have the authority to create IT centers of excellence, comprised of IT specialists from the various directorates. The office of the CIO would manage the centers as a means of delivering DHS-wide IT capabilities and resources.

The tasks outlined above will take some time to plan and accomplish. However, once in place, all IT resources and assets would be under the control of the DHS

CIO. Although there are many obstacles to overcome, the plan is expected to result in significant cost savings and greater consistency and efficiency by eliminating wasteful duplication, streamlining operation, and increasing accountability. In addition, the consolidations would help eliminate existing organizational stovepipes and help build a department culture that is vital to the long-term success of the agency.

Recommendations

The OIG recommends that, in keeping with legislative requirements and effective practices of other federal IT organizations, the Deputy Secretary:

1. Implement plans for centralizing IT support services.

2. Reposition the CIO to report directly to the Office of the Deputy Secretary, thereby providing the CIO with the authority and the ability to influence senior executive decisions concerning department-wide IT investments and strategies.

3. Document and communicate the roles of component level CIOs, including their dual reporting relationships to the DHS CIO and heads of their respective DHS organizations, thereby ensuring their support for and alignment with central policies, standards, and strategies for consolidating and integrating the department's IT infrastructure as well as mission and business objectives.

4. Provide the DHS CIO office with the staff resources necessary to facilitate accomplishment of department-wide IT consolidation objectives and supporting initiatives, including IT planning; policy and standards formation; enterprise architecture development; network management; information assurance; and, technical, business and administrative support.

5. Assign the CIO a key role in all levels of the department's investment review process to ensure, guide, and document timely and effective IT investment decisions to support accomplishment of department-wide business objectives.

Management Comments and OIG Evaluation

We obtained written comments on a draft of this report from the Deputy Secretary. We have incorporated the comments where appropriate and included a copy of the comments in their entirety at Appendix B.

The Deputy Secretary concurred with Recommendations 1 and 3. Specifically, with regard to Recommendation 1, the Deputy Secretary said that the department would review further the Secretary's September 12, 2003, memorandum reflecting the intent to consolidate and integrate DHS-wide support functions, including the DHS CIO/CIO council plan for centralization. In response to Recommendation 3, the Deputy Secretary plans to establish formal reporting relationships between the DHS CIO and the CIOs of the major component organizations. The Deputy Secretary said that all departmental component CIOs will support the DHS CIO in all IT matters without exception, in addition to reporting to their respective agency heads. The formalized relationships and descriptions of duties will be published in the department's organization manual; interim guidance will be provided as needed. The OIG views these plans as positive steps toward improving enterprise-wide IT management and looks forward to their implementation.

The Deputy Secretary neither concurred nor disagreed with Recommendation 4 with regard to supplying the DHS CIO Office with needed staff resources. The Deputy Secretary said that the department is constantly striving to provide optimal resources throughout all DHS components and will look for further opportunities to re-program critical resources and personnel during the centralization process. The OIG appreciates the Deputy Secretary's intentions to optimize resources across DHS components. However, the OIG encourages more immediate attention to supplying the CIO office with the staff it needs to carry out its department-wide responsibilities. The CIO has the enormous task of creating one network and one infrastructure to ensure IT connectivity among the department's 22 legacy organizations. The OIG is concerned that the small CIO office staff of 49 is woefully inadequate to meet the many challenges of providing IT services, technology systems, facilities, and initiatives to support an organization of 180,000 employees. Without the proper staffing, the Office of the CIO has been hindered in putting in place the plans, guidance, and standards needed for critical functions such as information security and wireless communications.

For example, based on its annual evaluation of DHS efforts to meet FISMA requirements, the OIG reported in September 2003 that none of the components had a fully functioning IT security program, only 37 percent of DHS systems had

been certified and accredited, and only 39 percent had been assessed for risk.[11] Further, in June 2004, the OIG reported that DHS had an incomplete wireless security policy and inadequate procedures to implement a DHS Wireless Security Program.[12]

Similarly, the Deputy Secretary neither concurred nor disagreed with Recommendation 5 that the DHS CIO play a greater role in investment decision-making. The Deputy Secretary countered that the CIO is already an integral member at all levels of the IT investment review process. The OIG does not agree. Although the CIO may be a participant at each of the department's four investment review levels, the CIO does not have the power and authority required by the Clinger-Cohen Act to control all IT investments department-wide. For example, the CIO does not have the final authority regarding major, mission critical IT investments at Level 1 within the department. In one instance, the former Deputy Secretary overrode the CIO's recommendation to discontinue development of a costly, duplicative IT system. Further, the OIG identified instances where DHS components have developed IT systems without CIO guidance or authorization, creating further duplication and an inefficient use of IT resources.

In commenting on Recommendation 5, the Deputy Secretary also recommended adding the CIO as a member of the Level 2 Joint Requirements Council responsible for non-IT issues, thereby providing an element of crosscutting and situational awareness. The OIG views this planned action as a good start toward enhancing the CIO's involvement in the department's investment review process and awaits notification of its implementation. However, the OIG believes that more needs to be done to assign the CIO a key role at all levels of the department's investment review process.

Finally, the Deputy Secretary did not concur with Recommendation 2 to reposition the CIO to report directly to the Office of the Deputy Secretary. The Deputy Secretary said that the current arrangement in which the CIO reports directly to the Under Secretary for Management does not hinder or preclude the CIO from performing all essential job-related requirements. The Deputy Secretary said that the priorities of the Secretary, Deputy Secretary, and DHS are known throughout the chain of command and the responsible individuals have the inherent authority to accomplish these tasks.

[11] OIG-IT-03-02.

[12] *Inadequate Security Controls Increase Risks to DHS Wireless Networks*, Office of Inspector General, Department of Homeland Security, OIG-04-27, June 2004.

The OIG does not agree with the Deputy Secretary's response. Federal guidelines require that each executive agency position a CIO as a member of the senior executive team with the accountability and responsibility to manage IT across organizational units. By reporting to the Under Secretary for Management rather than to the Secretary, the DHS CIO is not a peer with the DHS Under Secretaries and component directors, and, as such, lacks the power and influence to advise senior executives on how best to implement and manage IT across the department. Also, as the Deputy Secretary acknowledged in the response to Recommendation 3, the CIO's relationships and duties are not clear and need to be formalized and published department-wide. Recognizing these limitations, notably the House Appropriations Committee proposed, in the department's FY 2005 appropriations bill, to modify the Homeland Security Act to require that the CIO directly report to the Secretary of Homeland Security instead of to the Under Secretary for Management. Without an additional organizational layer to which the CIO must report, the Committee expects DHS IT decisions to be made more expeditiously.

As part of its ongoing responsibility to assess the efficiency and effectiveness of departmental programs and operations, the OIG conducted a review of DHS' IT management structure. The objectives of the review were to determine whether the CIO is appropriately positioned and has a sound structure for managing department-wide IT systems and programs; and to evaluate how effectively the CIO is planning and managing IT investments to meet the department's current and future technology needs.

To review the effectiveness of DHS' IT management structure, the OIG researched and summarized IT laws and federal guidance applicable to CIO organizations and IT infrastructure management. The OIG also researched and reviewed background literature and prior Government Accountability Office reports on ensuring effective IT organizations.

The OIG then addressed its specific review objectives. First, the OIG met with the DHS CIO and his executive staff to discuss his role, organization, operations, and position within the department. The Chief of Staff told the OIG about the CIO's reporting relationships with the Under Secretary for Management and other members of the senior executive team. The OIG met with the chief procurement officer, the chief human resources officer, and a chief financial officer representative to discuss working relationships between the CIO and his peers within the Management Directorate.

CIOs of each of the DHS component organizations told the OIG about their individual IT management environments, CIO reporting relationships, experiences as part of the CIO Council, and coordination with line of business systems owners. The OIG also met with former component-level CIOs to discuss their experiences in managing IT at DHS, concerns about attrition, and transitions to incoming CIO leadership. Budget officers and other managers within the Office of the CIO discussed IT budgeting, acquisition processes, IT and architectural planning, performance measurement, and policy and standard setting. Based on these interviews, the OIG performed an analysis of whether the CIO effectively communicates enterprise-wide IT strategies, goals, and objectives to senior managers, peers, IT officials, line managers, and subordinates. In addition, the OIG met with three federal agencies to conduct a best practices study and compare the DHS IT organization to the CIOs at these agencies.

To address the second objective of assessing the effectiveness of the department's IT investment management, the OIG reviewed directives and other available documentation that outlined these processes. The OIG met with budget officials

and chief financial officer representatives to gain a broader understanding of how these processes work within the department. CIOs, IT officials, and program officials within the individual component organizations told the OIG about specific IT investments and how they were controlled within the department. Officials within the office of the CIO and the budget office also provided an overview of the department's investment review processes and gave the OIG copies of the department's budget documents for FY 2005. These officials told the OIG about the various managers and forums involved in IT investment review and decision-making. Representatives of the various working groups, boards, and committees provided details on how these forums function. Lastly, the OIG examined business cases for selected IT projects to assess coordination and communication between IT managers and business owners.

The OIG conducted this review from October 2003 to May 2004 at various DHS headquarters and component organizations, and other federal agencies in the Washington, D.C metro area. The OIG limited its review to unclassified systems and processes and did not focus on sensitive systems or information. The OIG performed its work according to generally accepted government auditing standards.

The prinicipal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, (202) 254-4100; and Sondra McCauley, Director, Information Management, (202) 254-4212. Major OIG contributors to the audit are identified in Appendix C.

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

Homeland Security

July 20, 2004

MEMORANDUM FOR: CLARK KENT ERVIN
INSPECTOR GENERAL

FROM: J. M. LOY, ADM

SUBJECT: RE: DRAFT AUDIT REPORT – *IMPROVEMENTS NEEDED TO DHS' INFORMATION TECHNOLOGY MANAGEMENT STRUCTURE (A-IT-04-002)* DTD 24 JUNE 2004

Thank you for providing a draft copy of the report by the Office of Inspector General entitled, "Draft Audit Report – Improvement Needed to DHS' Information Technology Management Structure (A-IT-04-002)" dated June 24, 2004. We appreciate the opportunity to review, comment, and discuss the issues, findings and recommendations contained therein.

Information technology infrastructure, systems, management and support combine to form a pillar responsible for supporting the successes of the entire department as we conduct our demanding, diverse missions. Being critical to the effective and efficient performance of our duties, it is and will continue to be of highest priority with the most senior department leadership.

The attachment to this memorandum provides our detailed responses to the findings and recommendations in the subject report.

If you have any questions, please contact Tom Paar at (202) 282-8359.

Attachment

www.dhs.gov

Response to the
Draft Audit Report – *Improvements Needed to DHS' Information Technology Management Structure (A-IT-04-002)* dated 24 June 2004

Recommendation #1: Implement plans for centralizing Information Technology (IT) support services.

Response: Concur with findings that centralizing Department of Homeland Security (DHS) IT support services would benefit the department as a whole. In accordance with the Secretary's memo of September 12, 2003 reflecting intent to consolidate and integrate DHS-wide support functions, we will further review the Under Secretary of Management decision memorandum, including the DHS chief information officer (CIO)/CIO council plan for centralization.

Recommendation #2: Reposition the CIO to report directly to the Office of the Deputy Secretary, thereby providing the CIO with the authority and the ability to influence senior executive decisions concerning department-wide IT investments and strategies.

Response: Submit that DHS CIO does not need to report directly to the Secretary/Deputy Secretary and that reporting directly to the Under Secretary for Management does not hinder or preclude the CIO from performing all essential job related requirements. The priorities of the Secretary, Deputy Secretary and DHS are known throughout the chain of command and the responsible individuals have the inherent authority to accomplish these tasks.

Recommendation #3: Document and communicate the roles of component level CIOs, including their dual reporting relationships to the DHS CIO and heads of their respective DHS organizations, thereby ensuring their support for and alignment with central policies, standards, and strategies for consolidating and integrating the department's IT infrastructure as well as mission and business objectives.

Response: Concur with establishing formal reporting relationship between DHS CIO and CIO's of major component organizations. All departmental component CIO's will support the DHS CIO in all IT matters without exception, in addition to reporting to their respective agency heads. Formalized relationships and description of duties will be published in department organization manual. Interim guidance will be provided as needed.

Recommendation #4: Provide the DHS CIO office with the staff resources necessary to facilitate accomplishment of department-wide IT consolidation objectives and supporting initiatives, including IT planning; policy and standards formation; enterprise architecture development; network management; information assurance; and, technical, business and administrative support.

Response: Noted. We continue to strive to provide optimal resources throughout all DHS components. We will further look for opportunities to re-program critical resources/personnel during the centralization process.

Recommendation #5: Assign the CIO a key role in all levels of the department's investment review process to ensure, guide, and document timely and effective IT investment decisions to support accomplishment of department-wide business objectives.

Response: The DHS CIO is already an integral member at each level of the IT investment review process. In addition to establishing and heading the Enterprise Infrastructure Board, the CIO chairs the Level 3 Enterprise Architecture Board and is a voting member of both the Level 2 Management Review Council and the Level 1 Investment Review Board, and as such will always have significant input as to the management of the IT investment process. Recommend also adding the CIO as a member of the Level 2 Joint Requirements Council (non-IT issues) to provide an element of cross-cutting and situational awareness.

Frank Deffer, Assistant Inspector General, Information Technology Audits;
Sondra McCauley, Director, Information Management Division;
Ann Brooks, IT Audit Manager;
Timothy Walton, IT Auditor; and
Meghan Parker, IT Auditor.

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Under Secretary for Management
Chief Information Officer
DHS OIG Liaison
DHS Public Affairs

Office of Management and Budget

Homeland Security Bureau Chief
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) 254-4100, fax your request to (202) 254-4285, 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 the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.