Department of Homeland Security
Office of Inspector General

Immigration and Customs Enforcement Information Technology Management Progresses But Challenges Remain

OIG-10-90

May 2010

Office of Inspector General

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

Homeland
Security

May 28, 2010

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 addresses the strengths and weaknesses of Immigration and Customs Enforcement information technology management. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. 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.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary 1

Background 2

Results of Audit 5

IT Strategic Planning and Budgeting Processes Need Improvement 5

IT Investment Management Processes Need Improvement... 11

The OCIO Is Challenged to Achieve Effective Management of Agency-wide IT............ 17

Recommendations.. 24

Management Comments and OIG Analysis……………………………..………………......24

Appendixes

Appendix A: Objective, Scope and Methodology 26
Appendix B: Management Response to Draft Report 28
Appendix C: Major Contributors to the Report... 30
Appendix D: Report Distribution 31

Abbreviations

AD	Acquisition Directive
CIO	Chief Information Officer
DHS	Department of Homeland Security
FY	Fiscal Year
GAO	Government Accountability Office
ICE	Immigration and Customs Enforcement
IT	Information Technology
ITSR	Information Technology Service Request
MD	Management Directive
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
PEO	Program Executive Office
SELC	Systems Engineering Life Cycle
SLA	Service Level Agreement

Figures

Figure 1: ICE Organizational Structure 3
Figure 2: ICE OCIO Organizational Structure 3
Figure 3: OCIO Strategic Plan Goals 6
Figure 4: IT Strategic Plan Goals...7

Figure 5: Total ICE IT Spending, FY 2009 9

Figure 6: Comparison of DHS MD 1400 and DHS AD 102-01 IT Investment Levels 12

Figure 7: Proposed ICE OCIO Investment Management Structure....................13

Figure 8: High-Level ICE Life Cycle Management Process 15

Figure 9: IT Service Requests Since 2007 19

Figure 10: Total FY 2009 OCIO Funding by Fund Source 21

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

We audited Immigration and Customs Enforcement's information technology management functions. Our objective was to determine whether the components information technology management approach adequately addresses strategic planning, implementation, and management of technology to support its immigration and customs enforcement goals.

Immigration and Customs Enforcement has improved its strategic planning by implementing an Office of the Chief Information Officer organizational strategic plan. However, it has not yet finalized its information technology strategic plan to define key goals and objectives for fulfilling its mission responsibilities. Further, although the Office of the Chief Information Officer has oversight of information technology spending, its budget planning process did not capture all component information technology needs.

The Office of the Chief Information Officer is refining its information technology investment management and governance approach to improve oversight capabilities. The Office of the Chief Information Officer has also instituted a process for information technology life cycle management to oversee technology projects. However, extensive documentation preparation and review for information technology projects of all sizes, combined with a need for system life cycle management training, may hinder efficient management of information technology projects. Further, the Office of the Chief Information Officer is challenged to deliver effective information technology services and support due to conflicting priorities and staffing shortages. The Office of the Chief Information Officer is also unable to provide customers with details on program funds, and has not finalized information technology policies necessary for effective management of information technology activities.

Background

Immigration and Customs Enforcement (ICE) is the largest investigative arm of the Department of Homeland Security (DHS). ICE's mission is to "protect the security of the American people and homeland by vigilantly enforcing the Nation's immigration and customs laws." To accomplish this mission, ICE deters, interdicts, and investigates threats; combats cross-border and financial crime; and protects federal government facilities.

ICE has more than 400 offices and 20,000 employees in the United States and around the world. For fiscal year (FY) 2009, ICE had a budget of approximately $5.9 billion. This represents roughly 11% of DHS' overall FY 2009 budget of $52 billion.

ICE has two primary organizational units, the Office of the Deputy Assistant Secretary for Operations and the Office of the Deputy Assistant Secretary for Management. The Office of the Deputy Assistant Secretary for Operations provides leadership and coordination between the operational components to achieve agency goals. The Office of the Deputy Assistant Secretary for Management is responsible for coordination of the administrative and managerial components, as well as providing an integrated information technology (IT) infrastructure. These components, pictured in figure 1, are responsible for executing ICE's mission.

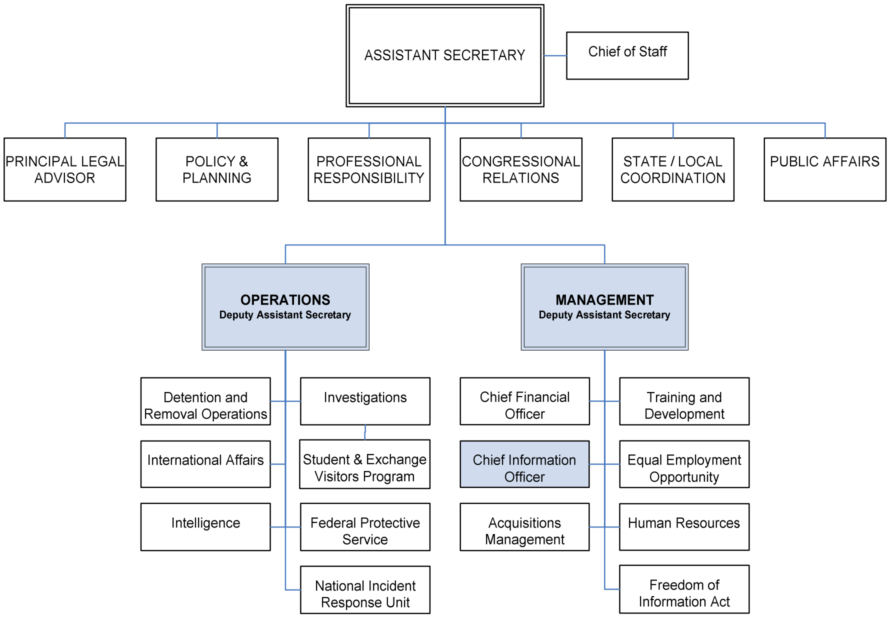

ASSISTANT SECRETARY
Chief of Staff
PRINCIPAL LEGAL ADVISOR
POLICY & PLANNING
PROFESSIONAL RESPONSIBILITY
CONGRESSIONAL RELATIONS
STATE / LOCAL COORDINATION
PUBLIC AFFAIRS
OPERATIONS Deputy Assistant Secretary
MANAGEMENT Deputy Assistant Secretary
Detention and Removal Operations
Investigations
International Affairs
Student & Exchange Visitors Program
Intelligence
Federal Protective Service
National Incident Response Unit
Chief Financial Officer
Training and Development
Chief Information Officer
Equal Employment Opportunity
Acquisitions Management
Human Resources
Freedom of Information Act

Figure 1: ICE Organizational Structure

Under the Deputy Assistant Secretary for Management, the Office of the Chief Information Officer (OCIO) provides information technology (IT) services and solutions in support of the ICE mission. Since 2005, the OCIO has improved its organizational and operational effectiveness by restructuring itself to align with the overall ICE mission, current operational priorities, core business processes, and emerging IT needs. The OCIO is composed of 10 divisions and offices, staffed with approximately 380 federal employees, that work together to achieve the ICE mission. Figure 2 shows the organizational structure of the OCIO.

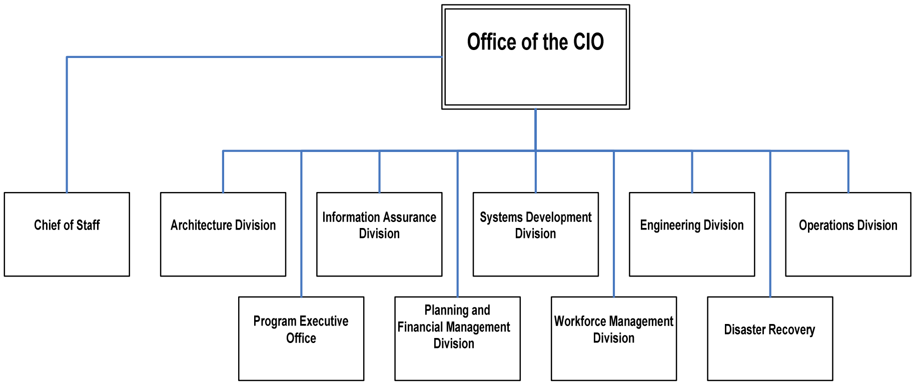


Figure 2: ICE OCIO Organizational Structure

Leveraging investigative techniques and IT resources are key factors in ICE's approach to accomplishing its mission. Technology plays a vital role for ICE, as evidenced by its FY 2009 IT expenditures of approximately $600 million. According to the *ICE Strategic Plan FY 2009–2013,* ICE's IT infrastructure needs to be modernized to help produce and share information that is accurate, secure, relevant, and timely. Accordingly, the OCIO has developed a number of critical IT initiatives to modernize IT systems and provide IT solutions to enable ICE personnel to meet their mission. For example, the Atlas program is an IT modernization and automation initiative that serves as the principal program to enhance ICE's technology foundation. The program acquires and integrates commercial-off-the-shelf hardware and software products into the ICE IT infrastructure to enhance core business functions. With this program, the OCIO aims to create, sustain, secure, and manage an IT environment to support the ICE law enforcement mission. ICE considers this program a key step toward improving internal information sharing.

Over the past several years, a number of audit reports have identified key IT challenges at ICE. In September 2005, the Government Accountability Office (GAO) reported that ICE's Atlas program had inadequate cost justification as well as insufficient program management practices, performance measurements, and expenditure plan.[1] In July 2006, GAO reported that ICE's Atlas project plans did not include essential elements, such as a work breakdown structure of tasks, identification of project costs, analysis of constraints and risks, and review and approval by management and stakeholders.[2] Finally, in April 2007, GAO reported that ICE had not implemented key system management practices that were needed to ensure that major programs, such as the Atlas program, would deliver IT infrastructure capabilities and benefits on time and within budget.[3]

In September 2008, we reported that although ICE was in the process of improving its IT management functions and operations, mature IT strategic planning and governance capabilities were needed.[4]

[1] *Management Improvements Needed on Immigration and Customs Enforcement's Infrastructure Modernization Program*, GAO-05-805, September 2005.
[2] *Immigration and Customs Enforcement Is Beginning to Address Infrastructure Modernization Program Weaknesses but Key Improvements Still Needed*, GAO-06-823, July 2006.
[3] *Immigration and Customs Enforcement Needs to Fully Address Significant Infrastructure Modernization Program Management Weaknesses*, GAO-07-565, April 2007.
[4] *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain*, OIG-08-91, September 2008.

Results of Audit

IT Strategic Planning and Budgeting Processes Need Improvement

ICE needs to improve its IT strategic planning and budget process. Although it has completed an OCIO organizational strategic plan and established an approach to measure workforce, business, and process effectiveness against that plan, these efforts do not address agency-wide IT-specific goals. Further, the OCIO developed a separate draft IT strategic plan that defines key goals and objectives for fulfilling ICE's mission responsibilities, but the completion of that plan is on hold until ICE updates its overall strategic plan. As a result, the OCIO cannot ensure that its IT initiatives are contributing fully to ICE mission goals.

The OCIO has taken steps to improve planning for all ICE programs by establishing an OCIO IT budget process. The OCIO reviewed and approved component IT spending throughout the year. However, the budget planning process did not fully represent what ICE spent on IT in FY 2009. As a result, the OCIO has limited ability to proactively manage and administer all IT resources and assets.

OCIO Strategic Planning

The *Government Performance and Results Act of 1993* holds federal agencies responsible for strategic planning to ensure efficient and effective operations and use of resources to achieve mission results.[5] Further, *DHS Management Directive (MD) 0007.1* requires agency Chief Information Officers (CIOs) to develop and implement an IT Strategic Plan.[6] The plan should clearly define how IT supports an agency's mission and drives investment decisions, guiding the agency toward its goals and priorities.

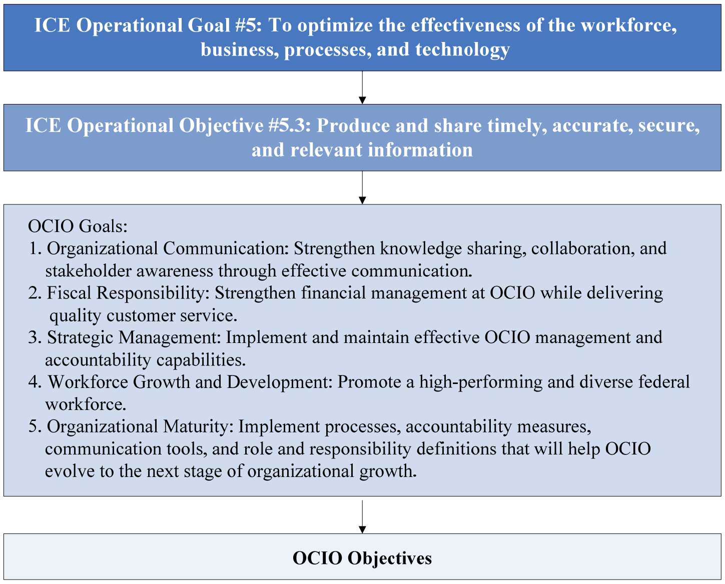
In 2009, the OCIO completed and implemented its first strategic plan—*OCIO Strategic Plan FY2009–FY2012*. The OCIO developed the plan to align with the operational goal in the *ICE*

[5] Public Law 103-62, August 3, 1993.

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

Strategic Plan FY2009–FY2013 to optimize the effectiveness of the workforce, business processes, and technology. According to the OCIO, this alignment will ensure that the OCIO Strategic Plan supports the agency's operational need for technology and provides direction for the OCIO's specific organization needs.

The OCIO Strategic Plan contains five goals, and corresponding objectives, aimed at developing and improving the OCIO organization. These goals, presented in figure 3, address communication, financial management, strategic management, workforce development, and organizational growth.



ICE Operational Goal #5: To optimize the effectiveness of the workforce, business, processes, and technology

ICE Operational Objective #5.3: Produce and share timely, accurate, secure, and relevant information

OCIO Goals:

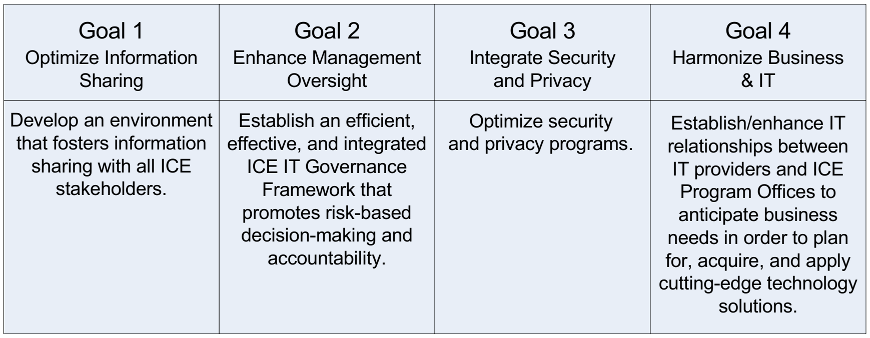
1. Organizational Communication: Strengthen knowledge sharing, collaboration, and stakeholder awareness through effective communication.
2. Fiscal Responsibility: Strengthen financial management at OCIO while delivering quality customer service.
3. Strategic Management: Implement and maintain effective OCIO management and accountability capabilities.
4. Workforce Growth and Development: Promote a high-performing and diverse federal workforce.
5. Organizational Maturity: Implement processes, accountability measures, communication tools, and role and responsibility definitions that will help OCIO evolve to the next stage of organizational growth.

OCIO Objectives

Figure 3: OCIO Strategic Plan Goals

The OCIO has established performance targets to ensure that it achieves its strategic goals throughout the year. These targets provide specific tasks for each OCIO division to achieve. For example, one division was tasked to "establish a Process Improvement Strategy and Governance Framework by September 30, 2009." Senior leadership tracks each division's progress in achieving the targets through annual performance plans and a performance status dashboard. As of September 30, 2009, the OCIO had achieved a "green" status for 86% of its objectives. Efforts are under way to draft new goals and objectives for FY 2010. According to OCIO management, these goals are being established collaboratively across the OCIO and will improve formal alignment with the DHS CIO goals.

The OCIO has drafted the *ICE IT Strategic Plan FY 2009–FY 2013* but has not yet finalized and implemented this plan. The plan has not been finalized because the ICE Strategic Plan, from which the IT plan should be derived, is being updated. At the completion of our fieldwork, the OCIO was waiting to receive the final ICE Strategic Plan before finalizing its IT plan. Although still in draft, the plan defines the ICE IT mission as providing "first class IT products and services to ensure ICE is able to effectively and efficiently accomplish its mission." The plan presents a framework for ICE to optimize the use of IT in support of DHS and ICE goals, objectives, and priorities. The IT Strategic Plan identifies four goals, as shown in figure 4.



Goal 1 Optimize Information Sharing	Goal 2 Enhance Management Oversight	Goal 3 Integrate Security and Privacy	Goal 4 Harmonize Business & IT
Develop an environment that fosters information sharing with all ICE stakeholders.	Establish an efficient, effective, and integrated ICE IT Governance Framework that promotes risk-based decision-making and accountability.	Optimize security and privacy programs.	Establish/enhance IT relationships between IT providers and ICE Program Offices to anticipate business needs in order to plan for, acquire, and apply cutting-edge technology solutions.

Figure 4: IT Strategic Plan Goals

The OCIO has developed specific objectives under each strategic goal. The goals and objectives will provide ICE managers and staff with the necessary direction for developing tactical and operational plans to meet ICE mission requirements. The OCIO expects that the IT strategic plan will enable ICE to fulfill its mission responsibilities and the OCIO to move forward in a defined strategic direction.

Without an overarching IT strategic plan and the tactical and operational plans that should flow from it, the OCIO cannot ensure that its IT projects, initiatives, and investments are contributing to ICE mission goals. Officials in ICE component offices told us that they are not clear on the direction the OCIO is taking to better serve mission operations. In addition, IT project managers said that they are not aware of an agency-wide IT vision that drives day-to-day work. Rather, work is prioritized on the basis of customer-driven requests and available funding. For example, ICE acquisitions officials said that procurements are often handled in the order they are received rather than by mission priorities.

IT Budget Process

The *Clinger-Cohen Act* requires that CIOs review the IT budget within their agency to effectively manage technology systems and initiatives as strategic investments.[7] Further, *DHS MD 0007.1* requires component CIOs to effectively manage and administer all IT resources and assets and prepare an IT budget for all component office IT activities.[8]

The OCIO has taken steps to improve budget planning for ICE IT programs. Specifically, the OCIO has established a budget process to identify and prioritize IT needs and implement a consolidated budget execution plan for IT resources supporting ICE's mission and goals. However, the FY 2009 IT budget plan did not capture all funds ICE component offices spent on technology. Although the OCIO has oversight of component office IT spending, it does not review and approve component IT plans at an earlier stage within the process. As a result, the OCIO is not able to guide IT purchases to promote standardization or strategic direction of agency technology.

IT Budget Process Established

The OCIO is responsible for estimating all funding needed for agency IT capabilities. To accomplish this, the OCIO has established a process to develop an annual IT budget plan. It begins this process by estimating the total expenses for all OCIO divisions using the prior year budget as a baseline. Building on this baseline, each division develops an updated budget plan that reflects its needs. The OCIO Budget Execution Office validates the divisional estimates and consolidates the plans into the OCIO budget execution plan.

The OCIO works with the ICE Budget Office and ICE components to identify the funding needed for agency-wide IT initiatives, equipment and services for the year. ICE component funding requests for major programs are captured in the annual IT service assessment process. During the budget process, the OCIO also considers plans for new IT initiatives from the annual Office of Management and Budget's Exhibit 300 business case summaries and new IT projects identified by ICE governance boards.

[7] Public Law 104-106, February 10, 1996.
[8] Department of Homeland Security, Management Directive 0007.1, *Information Technology Integration and Management*, March 15, 2007.

The OCIO compiles a budget execution plan that details the funding that can be spent on specific programs and projects for the year. The OCIO and the ICE Budget Office review and prioritize these requests to ensure alignment with agency goals. According to the OCIO, this collaboration between the OCIO and the ICE Budget Office ensures that all IT needs are captured in the OCIO annual budget process.

IT Spending Outside of Budget Process

Although the OCIO FY 2009 budget accounted for all OCIO-managed funds, it did not account for all ICE IT funds spent during the year. In FY 2009, the OCIO was able to account for 87% of the IT funds through its consolidated budget formulation process, as shown in figure 5.

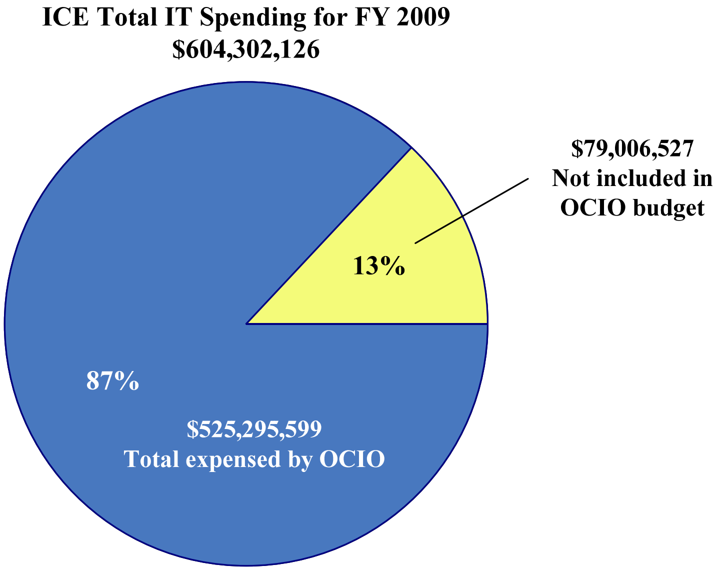


Figure 5: Total ICE IT Spending, FY 2009

The OCIO has established formal processes to monitor component spending on IT equipment and services. According to the OCIO, regardless of who funds the requisition, IT equipment purchases are made through a standard IT Service Request (ITSR) process. In this process, ICE component offices submit requests for IT purchases to the OCIO for approval by the CIO.

Acquisitions for IT services are also subject to formal OCIO oversight. The OCIO has instituted an acquisition review process to ensure IT acquisitions are reviewed before they are completed. This process provides a standard mechanism for ICE to initiate investment reviews to ensure compliance with the DHS-level acquisitions guidance and review process. According to the OCIO, the review process also helps to ensure alignment of investments with ICE and DHS strategic goals.

Although the OCIO maintains awareness of IT spending through the ITSR and acquisition review processes, these processes do not provide an opportunity for the OCIO to conduct a complete review of component office IT plans prior to spending. As a result, the OCIO has limited ability to effectively manage and administer all IT resources and assets with a complete and accurate budget. Consequently, the ability of OCIO to consolidate purchases, promote IT standardization, and achieve tighter control of IT expenditures is hindered.

IT Investment Management Processes Need Improvement

The OCIO is refining its IT investment management approach in response to recent changes in DHS acquisitions requirements. Specifically, the OCIO is instituting new IT governance boards and has developed a formal governance process. The OCIO expects the new governance process to provide a more formal structure for IT investment review and to increase oversight for OCIO-managed programs.

OCIO's system life cycle management process plays a key role in ensuring that ICE IT projects receive the appropriate level of review and oversight. Although the OCIO has established a system life cycle management process to oversee all ICE technology projects, IT managers are challenged to achieve efficient oversight because of the number of documents required for IT projects of all sizes. Further, ICE components do not know how to apply the process to their projects, in part because of a lack of training. As a result, IT projects may incur increased costs.

IT Investment Management Approach Refined

According to federal guidance, the CIO is required to implement IT governance structures and to ensure effective acquisition of IT resources.[9] Additionally, according to *DHS MD 0007.1*, the component CIO is responsible for the effective management and administration of all IT resources and assets by reviewing and approving IT acquisitions in accordance with DHS policies and guidance.

In November 2008, DHS issued Acquisition Directive (AD) 102-01.[10] The directive defines the acquisitions process that must be followed for IT projects to receive funding. This directive establishes three investment levels and defines department and component review and approval authority for each level. Figure 6 shows these thresholds and responsibilities.

[9] The *Clinger-Cohen Act of 1996*; OMB Circular A-130, *Management of Federal Information Resources*; and OMB Circular A-11, *Planning, Budgeting, Acquisition and Management of Capital Assets* provide regulations and guidance for investment review and capital planning activities.
[10] DHS AD 102-01, Version 1.9, *Acquisition Directive*, 7 Nov. 2008.

	Previous Requirements (DHS MD 1400)[11]		**DHS AD 102-01**	
Project Level	**Investment Threshold** (total life cycle costs)	**Review/ Approval**	**Investment Threshold** (total life cycle costs)	**Overseen by**
Level 1	> $200M	DHS	≥ $1B	DHS
Level 2	$20M – $200M	DHS	$300M – $1B	DHS
Level 3	$5M – $20M	DHS	< $300M	ICE

Figure 6: Comparison of DHS MD 1400 and DHS AD 102-01 IT Investment Levels

The new departmental acquisitions guidance has increased the number of IT projects that require ICE-level review and approval. Previously, DHS held review and approval authority for all IT investments with total life cycle costs of greater than $5 million. However, under AD 102-01, DHS now reviews IT investments with life cycle costs of $300 million or more, with ICE responsible for reviewing and approving all IT investments of less than $300 million.

To address the requirements of AD 102-01, the OCIO is updating its governance structure. It is instituting two new OCIO-level IT governance boards: the Cross-Impact Review Board and the Executive Board. These boards will provide a more formal structure to ensure acquisition oversight of ICE investments throughout their life cycle. These boards will meet weekly or monthly to review program and project accomplishments and plans during the acquisition process. Figure 7 shows the proposed governance structure with investment review responsibilities.

[11] Department of Homeland Security, Management Directive 1400, *Investment Review Process.*

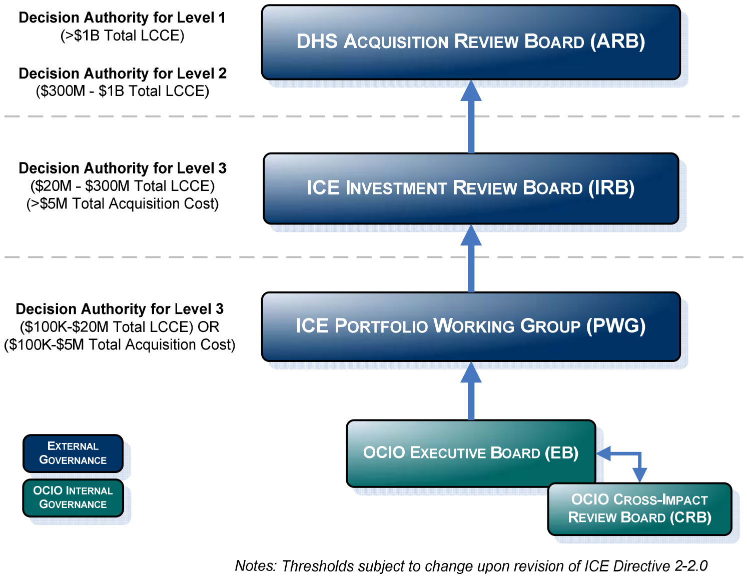

Decision Authority for Level 1
(>$1B Total LCCE)
Decision Authority for Level 2
($300M - $1B Total LCCE)
DHS Acquisition Review Board (ARB)
Decision Authority for Level 3
($20M - $300M Total LCCE)
(>$5M Total Acquisition Cost)
ICE Investment Review Board (IRB)
Decision Authority for Level 3
($100K-$20M Total LCCE) OR
($100K-$5M Total Acquisition Cost)
ICE Portfolio Working Group (PWG)
External Governance
OCIO Internal Governance
OCIO Executive Board (EB)
OCIO Cross-Impact Review Board (CRB)
Notes: Thresholds subject to change upon revision of ICE Directive 2-2.0

Figure 7: Proposed ICE OCIO Investment Management Structure

The Cross-Impact Review Board is responsible for facilitating analyses, providing guidance, and making recommendations for acquisitions to the Executive Board. The Cross-Impact Review Board, made up of management-level subject matter experts representing ICE/OCIO's core functions, will support and report to the Executive Board.

The Executive Board is the decision-making body that is responsible for reviewing and approving Cross-Impact Review Board recommendations. The Executive Board is made up of ICE/OCIO division directors and will support and report to the existing ICE Portfolio Working Group.

To provide an overarching structure for the new boards, the OCIO developed a formal governance process in 2009. The new process describes each governance board and illustrates the interactions between OCIO-level and ICE-level boards. The process also defines three governance sub-processes: acquisition management, management reviews, and process asset management. The OCIO expects the new governance process to provide a more formal review structure for IT investments and to increase oversight for programs.

In February 2009, the new boards began a piloting phase to test investment management processes with a select number of IT projects. For example, the Traveler Enforcement Communication System modernization program, an effort to modernize the system that screens travelers entering the United States, went through all levels of review with the two new OCIO-level boards. The boards tracked all comment forms, meeting minutes, and action items so that the decisions they made could be clearly communicated to the programs. According to the OCIO, the pilot phase provided a complete picture of the end-to-end governance process. At the conclusion of our review, the OCIO was updating each governance board's charter based on lessons learned from the pilots. The OCIO expected to implement the new boards in February or March 2010 after governance charters were finalized.

Although the OCIO is documenting and communicating guidance on its new investment review process, challenges remain for successful implementation of the process. According to several ICE officials, project managers are not consistently aware of the OCIO review boards and have limited understanding of the decision-making process. Further, many project managers do not clearly understand what is required for the new acquisition process. For example, most project managers said they do not always understand when or how to enter the formal review process or what documentation is required.

Systems Life Cycle Management Process Established

An essential part of AD 102-01 is the DHS Systems Engineering Life Cycle (SELC) set forth in appendix B of the directive. The purpose of the DHS SELC Guide is to standardize the system life cycle process across DHS. The guide is designed to ensure that appropriate activities are planned and implemented in each phase of the life cycle to increase a project's success.

The OCIO has recently aligned its system life cycle management process with the DHS SELC. ICE established the process to oversee the various technical, security, and quality aspects of its technology projects and to manage the integration of technology into ICE. The life cycle management process consists mainly of a set of nine activities, documents, technology artifacts, and gate reviews that can be customized to fit the unique needs of a project. Figure 8 depicts the nine activities, also referred to as phases.

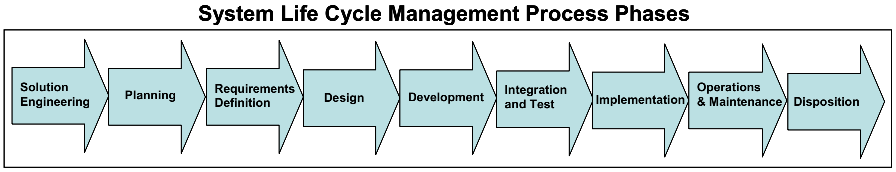


Figure 8: High-Level ICE Life Cycle Management Process

During the process, the project team completes the required activities. The results of the activities are recorded in documents and technology artifacts such as code. The documents and technology artifacts are assessed for adherence to ICE standards and guidelines and evaluated in gate reviews to determine how the project should proceed.

Documentation Requirements for IT Projects

Although the life cycle management process is accepted as the agency's standard approach, IT and component personnel said that the volume of documents required for small projects is excessive, increasing the workload for administering IT projects. Specifically, IT project managers said the same documentation is required for all IT projects reviewed by either DHS or ICE. The ICE IT life cycle handbook specifies that a range of up to 60 documents may be required throughout the project, depending on the project's scope and complexity. OCIO project managers are concerned about the potential impact on cost and schedule for current IT projects. One IT project manager explained that a small IT project may incur a significant cost increase in order to complete required documentation. As a result, the OCIO is challenged to deliver IT solutions in a cost-effective or timely manner.

Although the life cycle management process can be tailored based on a project's size, scope, and risks, project managers said that the amount of documentation required remains burdensome across all project levels. To address these concerns, the OCIO has implemented a new Program Executive Office (PEO) to help program and project managers navigate system life cycle processes more efficiently. One of the initial efforts by the PEO was to simplify the IT life cycle process. The PEO offers assistance to the project manager to develop a Project Tailoring Plan in the first phase of the process. This plan documents the overall development approach for the program or project. However, IT managers said that an appropriate level of review activities and required documentation is not yet effectively tailored to the project investment size.

Clarity Needed for System Life Cycle Management Process

The process described within the ICE System Life Cycle Management Handbook applies to all ICE technology projects, including operational systems, infrastructure, and field technology initiatives, regardless of sponsor, developer, project size, methodology, or technology used. Thus, all ICE personnel and IT project teams must adhere to the ICE life cycle management process when developing or modifying ICE technology. However, ICE component office personnel said that they do not know how to apply the process to their IT projects. For example, when the Federal Protective Service began a project to automate existing manual processes, personnel did not know what documents were required during the initial phases of the project. Further, the IT project faced challenges when OCIO guidance did not clearly specify what was required from the ICE component personnel and contractors supporting the project team. This situation was compounded when requirements for documentation and gate reviews changed during the process due to a change in the project's investment level categorization.

Additionally, ICE customers working on an investment in excess of $50 million said they did not clearly understand how to prepare for required reviews throughout the process. Specifically, the project team did not know what documentation was required or how to plan the appropriate timeframes for each review. Further, the project team said that new documentation and review requirements, such as an architecture and design review, were introduced throughout the process.

ICE component officials said that personnel involved in the system life cycle management process needed training. Although life cycle management tutorials and templates are offered, training is not required for ICE component personnel. As a result, component personnel often proceed without an adequate understanding of the process. Further, project teams are unable to plan for needed staff and budget to ensure that activities are completed to keep the project on schedule.

The OCIO Is Challenged to Achieve Effective Management of Agency-wide IT

Although the OCIO has developed a structure to foster communications with its customers, ICE component offices are concerned that the OCIO does not understand their needs and priorities. As a result, component office officials may plan their own IT solutions without OCIO coordination. In addition, the ICE component offices we spoke with said that there was little transparency in how the OCIO spent their program funds, resulting in a lack of confidence related to IT funds management. In addition, ICE has not yet finalized and instituted a number of necessary IT policies. Without such policies, the OCIO does not have the controls in place to govern and manage IT activities.

IT Service Delivery Needs Improvement

According to *DHS MD 0007.1*, the component CIO is responsible for effective management and administration of all component IT resources and assets to meet mission, departmental, and enterprise program goals. The OCIO has developed an organizational structure to establish customer relationships while also providing centralized management of agency-wide IT. However, execution of several IT projects was hindered by insufficient understanding of customer needs and limited staff.

Systems Development Division

The OCIO established a Systems Development Division to focus on developing new ICE IT applications, enhancing and maintaining existing applications, and supporting IT program initiatives. Within this division, the OCIO established an account executive approach to foster customer relationships and ensure that it understands its customers' business needs. Account executives serve as customer service liaisons to the program offices in ICE. With this effort, the OCIO aims to improve its relationship with ICE component offices, as well as its ability to support the full IT life cycle of business applications.

At least five account executives work with ICE customers to understand their business needs and priorities and to vet new system requirements. Account executives told us that their roles and responsibilities include translating business requirements into technical solutions, as well as to help customers through the governance process. Account executives and OCIO IT project managers assist the customer through reviews and help to develop the documentation required for the process and acquisitions packages. IT project managers also attend project meetings with component office customers to foster continual engagement throughout the project.

Customer Needs

Some ICE customers said that they have not been able to obtain IT solutions to meet their mission operational needs. For example, the OCIO has restricted the use of wireless capabilities owing to the agency's involvement with law enforcement data. However, non-law enforcement programs within ICE find these protocols too constricting. The OCIO has denied their requests for IT capabilities, such as wireless Internet or "webinars," to collaborate with ICE component stakeholders. As a result, these customers do not believe that the OCIO understands their mission well enough to deliver IT solutions to support their operations.

Time and Resources

OCIO customers also said that there are often delays of 60 days or more in receiving responses to their IT requests. For example, one ICE component requested that a system be moved to another domain so it could support current IT program needs, a request the component felt should have been completed quickly. However, after the request had remained open for three months, the component director had to contact OCIO management to make this priority known. Another ICE component waited nearly a year for a response on a request for Microsoft SharePoint.

ICE customers we spoke with said that when the OCIO's response to their IT request is delayed beyond 60 days, it can cause significant setbacks to IT project efforts, as well as increased costs. For example, during one system development project, the customer needed an environment established for system testing. The OCIO was not able to respond in a timely manner. This resulted in missed deadlines for a project that was rated a top priority within the component office. In another case, one component had to spend an additional $200,000 on its project because it could not obtain a response from the OCIO on a connectivity request.

Because there is no defined review period for IT requests continues to introduce risks to IT projects. One ICE customer said that IT requests often remain open for three months or longer without resolution from the OCIO. In these cases, risks are identified and documented for mitigation. For example, one IT project identified at least seven high-priority issues and risks to the project schedule resulting from potential rework to redesign applications or to select alternate solutions.

OCIO customers said that the OCIO remains focused on its internal priorities, such as its workforce, business, and process effectiveness, rather than on its customers. Customers noted challenges in working with the OCIO because it had limited time and resources for customer IT projects. OCIO IT managers acknowledged that they are focused mainly on priorities, workload, and deadlines within their own division. IT staff also said that they are sometimes not readily available to work on customer issues because they are focused on division-specific activities.

Staffing

Staffing shortages present challenges to efficiently managing IT systems and development work. At the time of our audit, the OCIO had approximately 350 government employees and 1,860 contract employees. Although the OCIO has doubled its staffing level over the last two years, the workload has tripled over the same period. For example, ITSRs have increased from 982 to 3,629 from FY 2007 to FY 2009. Figure 9 shows the number of ITSRs for the past three years.

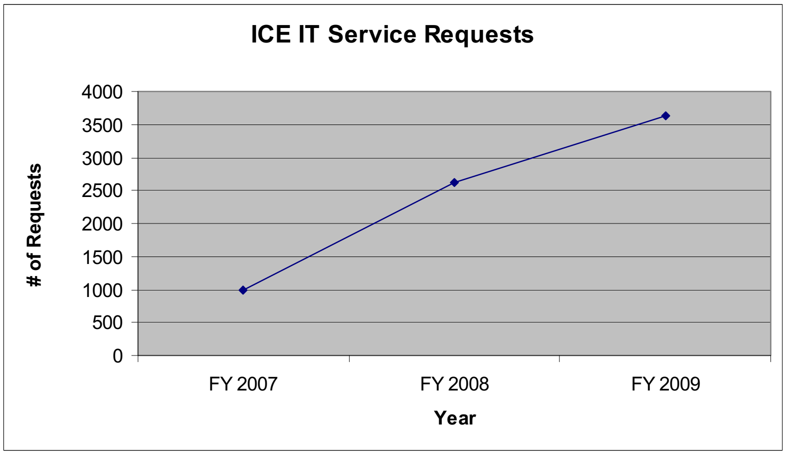


Figure 9: IT Service Requests Since 2007

Staff shortages are a critical issue for some OCIO divisions. For example, the System Development Division has only 81 federal employees to manage its approximately 140 system development projects. Although OCIO divisions augment their staff with contractors, only federal employees may manage IT projects. In some cases, there are not enough federal employees to manage the number of IT projects. For example, one branch is staffed with 11 federal employees and approximately 225 contractors. Another System Development division branch has approximately 80 projects, but only 20 federal employees to oversee all contractors and development activities.

As a result of the staffing shortage, project managers are stretched thin, each managing multiple projects. Consequently, OCIO divisions struggle to manage their current project workload and meet their customers' IT system needs. Staff shortages may also limit the OCIO's ability to meet new customer requirements. OCIO officials said they are in the process of determining appropriate contractor and federal employee staffing levels.

OCIO Management of Program Funds Is Not Transparent

DHS MD 0007.1 requires component CIOs to effectively manage and administer all component IT resources and assets. However, OCIO has not been able to provide component offices with detailed accounting of how their funds are being spent.

OCIO receives funds from ICE component offices for the IT services OCIO provides to them. ICE component offices enter into two types of IT service agreements with the OCIO—Service-Wide Agreements and Service-Level Agreements (SLAs). Service-Wide Agreements are primarily focused on common IT operations and maintenance services used across all ICE programs. For example, the OCIO provides ICE component offices with IT support for telecommunications, financial systems, and operations and maintenance of program systems and applications. ICE component offices use SLAs to obtain specific IT services to meet their unique IT needs. For example, the OCIO has an SLA with one component office to deliver IT equipment and contract services for infrastructure engineering assistance and other contractor support. Approximately 52% of the OCIO's FY 2009 funding was derived from these two types of service agreements, as figure 10 shows.

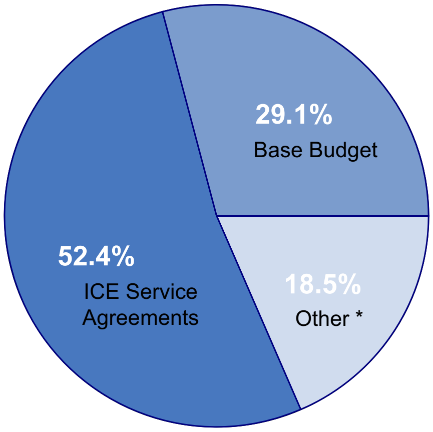


Figure 10: Total FY 2009 OCIO Funding by Fund Source

*Other includes appropriations received for, among other things, *Automation Modernization and Recovery Act* projects, as well as user fees received from external sources.

The ICE component office officials said that there was little transparency in how the OCIO spent their program funds. They said that they do not receive adequate reports from the OCIO on how service agreement funds are managed and spent, despite their requests for more information. Instead, the OCIO provides a statement that includes only the total dollar amount that the office provided to the OCIO and the total dollar amount spent. In addition, ICE officials said that the costs for IT service agreements often increase during the year, with little justification or details on how funds were spent. Further, the OCIO does not provide detailed spending reports for ongoing IT programs that it is managing. For example, one office received no details when the OCIO spent a multiyear budget for one of its IT programs in one year, and the cost of the program increased from $20 million to $50 million. Although the component office requested that the OCIO provide justification for the increase, the information was not provided.

OCIO officials said that they cannot easily provide component offices with detailed reporting on how service agreement funds are spent. The OCIO Budget Execution Branch uses the Federal Financial Management System to manage agency financial transactions. The branch can obtain some information, such as the amount of spending and the available balance on SLAs, from the system because SLAs are assigned individual project and other accounting codes. However, for more detailed information, such as which activities have been completed and the amount spent on each, the budget branch must obtain the information manually. It issues a data call once a month to OCIO project managers to obtain that information. In addition, tracking spending for Service-Wide Agreements is difficult because the funds received from all ICE component offices, which pay different amounts based on service utilization estimates, are combined into one "basket" and are not tracked by program.

Without more robust tracking and reporting capability, the OCIO is challenged to provide details on how ICE program funds are being spent. As a result, ICE component office officials do not believe they are receiving sufficient financial reporting from the OCIO. This fosters a lack of confidence that the OCIO is effectively managing the funds ICE component offices provide for IT services and initiatives.

IT Policies Are Needed to Support IT Management Functions

The *Clinger-Cohen Act* requires the ICE CIO to promote effective and efficient management and operations, as well as facilitate improvements to agency processes in regard to IT resources. Additionally, *DHS MD 0007.1* requires that the ICE CIO ensure alignment with DHS policies and procedures. IT policies are instrumental in ensuring that ICE IT system development and IT operations are executed in accordance with department and agency guidelines.

ICE has not yet published the IT policies needed to support and manage agency-wide IT. As of November 2009, fewer than one-third of the IT policies or directives recommended for development had been completed. Specifically, 16 IT policies or directives were in development—under review, pending signature, or on hold due to other circumstances. These policies address issues such as the IT procurement review, life cycle management, ITSR, and IT security. Additionally, three directives had been completed but not yet implemented while awaiting labor relations negotiations. A number of additional IT policies have been recommended for development but not yet begun. As a result, important guidance on agency-wide IT practices, such as IT security for remote access, has not yet been implemented.

OCIO officials said that a formal policy management framework has not yet been instituted within ICE. The existing review process for policy approval is lengthy, requiring that all draft policies be reviewed by multiple ICE stakeholders. Some policies have been in development for as long as three years because of this lengthy process. The OCIO has assigned a priority indicator to certain policies and directives that it considers the most critical. For example, an ITSR policy with an "A" level priority is the highest priority.

In the absence of completed and published IT policies, a number of critical IT management practices do not have formal support. For example, no policy gives PEO the authority to enforce compliance with the new standards and guidelines it is developing to improve IT management practices. Without enforcement authority, PEO can only encourage offices to use the tools it has developed for IT programs and projects. Because offices have the option of bypassing these tools, they run the risk of delays and problems that PEO's tools might have identified. In addition, OCIO's Information Assurance Division had to publish handbooks without official, signed policies in place because the information was needed quickly. Further, the directive requiring that all systems align with the ICE life cycle management process has not been finalized. As a result, the OCIO Architecture Division may be unable to enforce alignment, thus leaving the possibility for potential conflicts and misalignment with DHS guidance.

Recommendations

We are recommending that the ICE Assistant Secretary:

1. Finalize an agency-wide IT Strategic Plan to establish and communicate IT strategic goals and objectives to stakeholders.
2. Establish an agency-wide IT budget process to include all ICE component office technology initiatives and requirements.
3. Develop an OCIO staffing plan that includes specific actions and milestones for recruiting and retaining fulltime employees.
4. Establish a formal process to facilitate IT policy development, approval, and dissemination.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Acting Deputy Chief Financial Officer, ICE. In the comments, the Acting Deputy Chief Financial Officer concurred with our recommendations. We have included a copy of the comments in their entirety at Appendix B.

In response to recommendation 1, the Acting Deputy Chief Financial Officer stated that ICE has completed the ICE IT Strategic Plan as of April 9, 2010. Further, a revision of the plan is currently being developed to ensure alignment to DHS and ICE policy. The Acting Deputy Chief Financial Officer requested that Recommendation 1 remain open until the plan is completed in March 2011.

We recognize the progress made in this area since our review. We expect that ICE's IT Strategic Plan will help to ensure that IT initiatives fully support DHS and ICE strategic goals and objectives. We look forward to receiving a documented IT Strategic Plan.

In response to recommendation 2, the Acting Deputy Chief Financial Officer stated that the ICE OCIO is working with stakeholders to develop an IT budget process to include component input. The Acting Deputy Chief Financial Officer requested that

Recommendation 2 remain open until the Procurement Review Directive is approved in March 2011. We are encouraged by these plans and look forward to receiving the documented Procurement Review Directive.

In response to recommendation 3, the Acting Deputy Chief Financial Officer stated that the ICE OCIO is working to develop a staffing plan to address recruitment and retaining of full-time federal employees. The Acting Deputy Chief Financial Officer requested that recommendation 3 remain open until the staffing plan is finalized in December 2010. We are encouraged by this effort and look forward to receiving a documented staffing plan with specific actions and milestones for recruiting and retaining fulltime employees.

In response to recommendation 4, the Acting Deputy Chief Financial Officer stated that the ICE OCIO is in the process of developing a directive to enable tracking of policy requirements and status. The Acting Deputy Chief Financial Officer requested that recommendation 4 remain open until the policy directive is completed in December 2010. We are encouraged by this effort and look forward to receiving a documented directive which outlines how policy development will be managed.

As part of our ongoing responsibility to assess the efficiency, effectiveness, and economy of departmental programs and operations, we conducted a review of ICE to determine whether ICE's IT management approach adequately addresses strategic planning, implementation, and management of technology to support its goals.

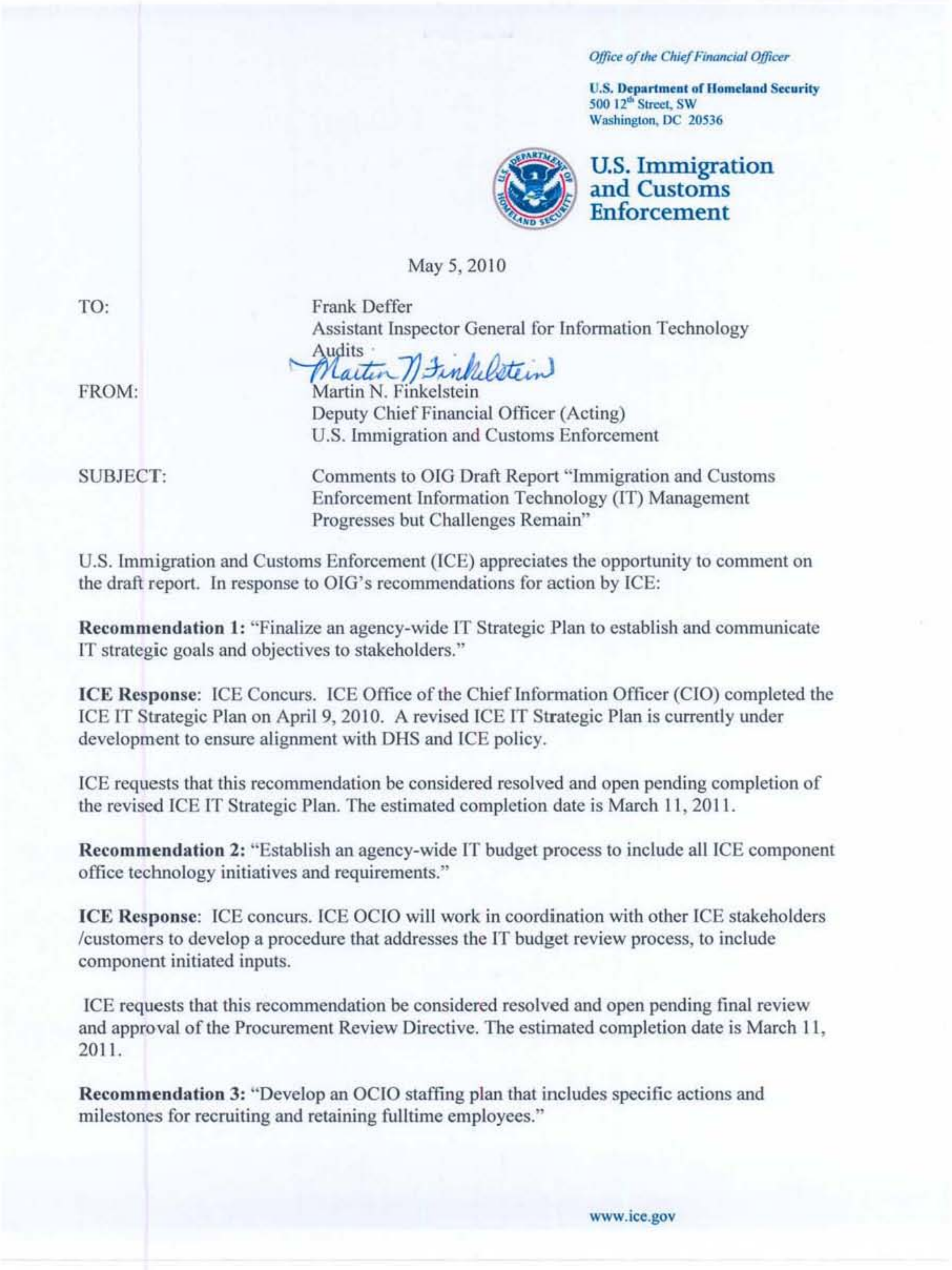
To establish criteria for this audit, we researched and reviewed federal laws and executive guidance related to IT management and CIO governance. We conducted research to obtain testimony, published reports, documents, and news articles regarding the DHS CIO operations and IT management throughout the department. Additionally, we reviewed recent GAO and DHS OIG reports to identify prior findings and recommendations. Using this information, we established a data collection approach that consisted of focused interviews and documentation analysis to accomplish our audit objectives. We then developed a series of questions and discussion topics to facilitate our interviews.

Subsequently, we held interviews at ICE headquarters and conducted teleconferences with ICE officials at field offices throughout the United States. Collectively, we interviewed more than 60 ICE headquarters and field management officials to learn about ICE's processes and IT management functions. At headquarters, we met with ICE OCIO officials, including the Deputy CIO, division directors, branch directors, and project managers, to discuss their roles and responsibilities related to ICE IT management and IT infrastructure modernization. We held teleconferences with ICE IT field operations area managers and IT specialists to understand IT management in the field. We discussed the current IT infrastructure and modernization efforts, local IT development practices, and user involvement and communication with headquarters. We collected supporting documents about ICE's IT structure, IT management functions, current initiatives, and future plans.

We conducted audit fieldwork from September to November 2009 at ICE headquarters in Washington, DC. We performed our work 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions, based on our audit objectives.

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

Appendix B
Management Response to Draft Report



Office of the Chief Financial Officer

U.S. Department of Homeland Security
500 12^{th} Street, SW
Washington, DC 20536

U.S. Immigration and Customs Enforcement

May 5, 2010

TO: Frank Deffer
Assistant Inspector General for Information Technology Audits

Martin N Finkelstein

FROM: Martin N. Finkelstein
Deputy Chief Financial Officer (Acting)
U.S. Immigration and Customs Enforcement

SUBJECT: Comments to OIG Draft Report "Immigration and Customs Enforcement Information Technology (IT) Management Progresses but Challenges Remain"

U.S. Immigration and Customs Enforcement (ICE) appreciates the opportunity to comment on the draft report. In response to OIG's recommendations for action by ICE:

Recommendation 1: "Finalize an agency-wide IT Strategic Plan to establish and communicate IT strategic goals and objectives to stakeholders."

ICE Response: ICE Concurs. ICE Office of the Chief Information Officer (CIO) completed the ICE IT Strategic Plan on April 9, 2010. A revised ICE IT Strategic Plan is currently under development to ensure alignment with DHS and ICE policy.

ICE requests that this recommendation be considered resolved and open pending completion of the revised ICE IT Strategic Plan. The estimated completion date is March 11, 2011.

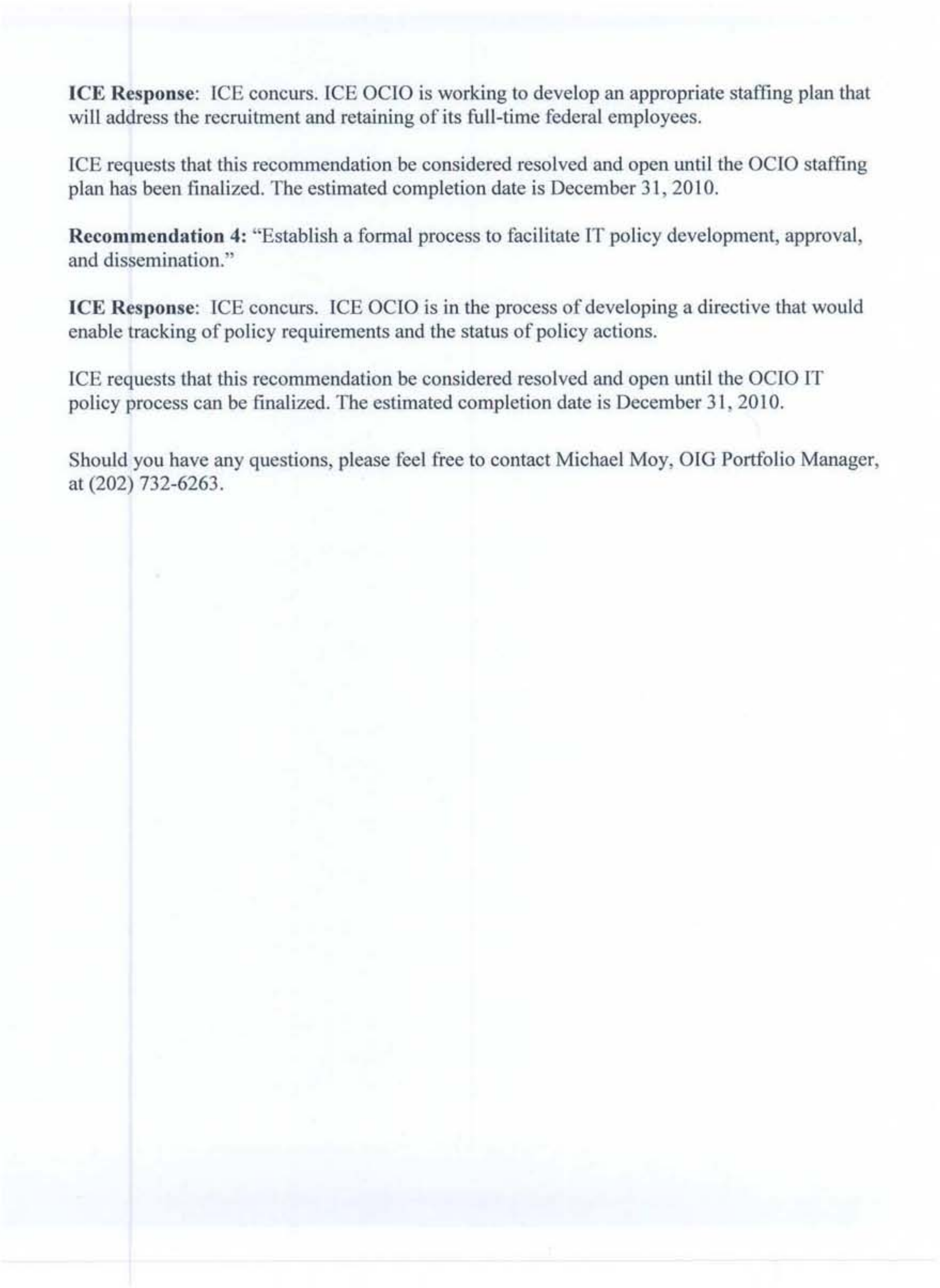
Recommendation 2: "Establish an agency-wide IT budget process to include all ICE component office technology initiatives and requirements."

ICE Response: ICE concurs. ICE OCIO will work in coordination with other ICE stakeholders /customers to develop a procedure that addresses the IT budget review process, to include component initiated inputs.

ICE requests that this recommendation be considered resolved and open pending final review and approval of the Procurement Review Directive. The estimated completion date is March 11, 2011.

Recommendation 3: "Develop an OCIO staffing plan that includes specific actions and milestones for recruiting and retaining fulltime employees."

www.ice.gov



ICE Response: ICE concurs. ICE OCIO is working to develop an appropriate staffing plan that will address the recruitment and retaining of its full-time federal employees.

ICE requests that this recommendation be considered resolved and open until the OCIO staffing plan has been finalized. The estimated completion date is December 31, 2010.

Recommendation 4: "Establish a formal process to facilitate IT policy development, approval, and dissemination."

ICE Response: ICE concurs. ICE OCIO is in the process of developing a directive that would enable tracking of policy requirements and the status of policy actions.

ICE requests that this recommendation be considered resolved and open until the OCIO IT policy process can be finalized. The estimated completion date is December 31, 2010.

Should you have any questions, please feel free to contact Michael Moy, OIG Portfolio Manager, at (202) 732-6263.

Information Management Division

Richard Harsche, Division Director
Kristen Evans, Audit Manager
Swati Nijhawan, Auditor
Melissa Keaster, Auditor
Erin Dunham, Auditor
Anna Tyler, Auditor
Karen Nelson, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Policy
Chief of Staff for Operations
Executive Secretary
General Counsel
DHS Chief Information Officer
DHS Chief Information Security Officer
ICE Assistant Secretary
ICE Chief Information Officer
ICE Audit Liaison
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
DHS Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Appropriate Congressional Oversight and Appropriations Committees

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 visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

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

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

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

- Email us at DHSOIGHOTLINE@dhs.gov; or

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

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