Department of Homeland Security
Office of Inspector General

Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology

OIG-11-69

April 2011

Office of Inspector General

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

Homeland Security

APR 01 2011

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 the Federal Emergency Management Agency's information systems. 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.

Frank Deffer
Assistant Inspector General
Information Technology Audits

Table of Contents/Abbreviations

Appendices

Abbreviations

ADD	Automated Deployment Database
CIO	Chief Information Officer
DHS	Department of Homeland Security
EADIS	Enterprise Application Development Integration Sustainment
EAO	Enterprise Architecture Office
EMMIE	Emergency Management Mission Integrated Environment
FEMA	Federal Emergency Management Agency
FY	fiscal year
GAO	Government Accountability Office
IFMIS	Integrated Financial Management Information System
IT	information technology
LIMS III	Logistics Information Management System III
LSCMS	Logistics Supply Chain Management System

Table of Contents/Abbreviations

MD	Management Directive
NEMIS	National Emergency Management Information System
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
SELC	Systems Engineering Life Cycle
TASC	Transformation and Systems Consolidation
TAV	Total Asset Visibility

List of Figures

Executive Summary

We audited the Federal Emergency Management Agency's efforts to provide the information systems needed to support its disaster response mission operations. The objective of our audit was to determine whether the agency's information technology modernization approach adequately addresses planning, implementation, and management to support efficient and effective disaster relief assistance. The scope and methodology of this audit are discussed further in Appendix A.

The agency's existing information technology systems do not support disaster response activities effectively. The agency has a number of information technology infrastructure modernization initiatives under way. However, it does not have a comprehensive information technology strategic plan with clearly defined goals and objectives or guidance for program office initiatives. In addition, it has not completed its efforts to document the agency's enterprise architecture. Without these critical elements, the agency is challenged to establish an effective approach to modernize its information technology infrastructure and systems.

In addition, the Office of the Chief Information Officer does not have an adequate understanding of existing information technology resources and needs throughout the agency. Specifically, the office does not have a complete, documented inventory of its systems to support disasters. Further, program and field offices continue to develop information technology systems independently of the office and have been slow to adopt the agency's standard information technology development approach. Finally, the office has completed improvements to its infrastructure foundation; however, efforts to modernize some of the agency's critical systems have been put on hold due to departmental consolidation plans. As a result, systems are not integrated, do not meet user requirements, and do not provide the information technology capabilities agency personnel and its external partners need to carry out disaster response and recovery operations in a timely or effective manner.

Background

The Federal Emergency Management Agency (FEMA) is the federal coordinator to prepare for, prevent, respond to, and recover from domestic disasters and emergencies. FEMA is responsible for saving lives and protecting property and public health and safety in a natural disaster, act of terrorism, or other manmade disaster. To support its mission, FEMA had a budget of approximately $10.5 billion for fiscal year (FY) 2010. This represents approximately 19% of the Department of Homeland Security's (DHS) overall budget of $55.1 billion.

FEMA has more than 3,700 full-time employees located at FEMA headquarters in Washington, DC, its ten regional offices, two area offices, five recovery offices, and various sites across the country. Additionally, FEMA has nearly 4,000 standby disaster assistance employees who are available for disaster deployment. FEMA also partners with other organizations that are part of the Nation's emergency management system, including 27 federal agencies, state and local emergency management agencies, and the American Red Cross.

FEMA consists of six primary components: Response and Recovery, Federal Insurance and Mitigation, Protection and National Preparedness, United States Fire Administration, Regional Operations, and Mission Support, as shown in figure 1. Each component has multiple directorates and program offices that carry out disaster response missions and functions, as well as administrative support.

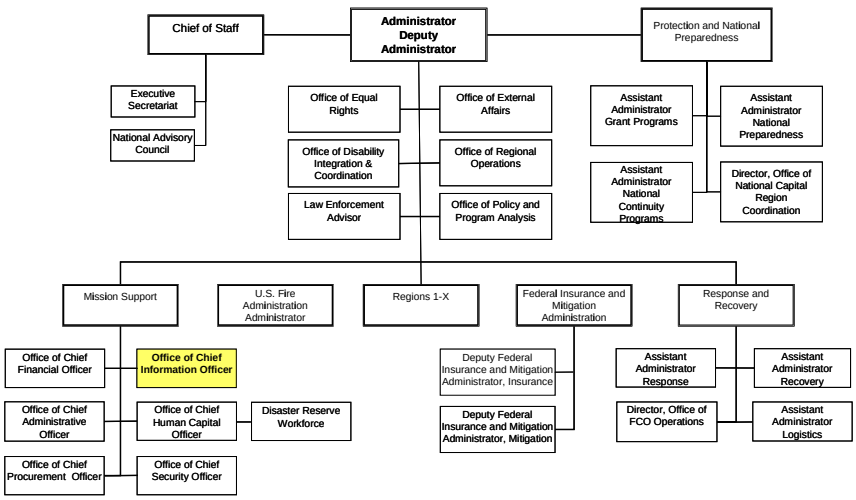

Figure 1: FEMA Organizational Structure as of September 2010

Within the Mission Support component, the Office of the Chief Information Officer (OCIO) is responsible for providing the information technology (IT) infrastructure to support FEMA's mission. In FY 2010, the FEMA OCIO employed nearly 500 federal employees and 319 contractors and had a budget of approximately $113 million. As shown in figure 2, the office is organized into two major divisions to administer IT functions and services.

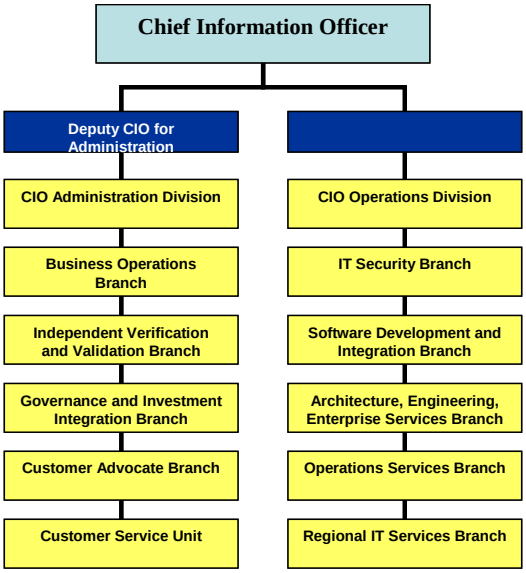

Figure 2: OCIO Organizational Structure as of May 2010

IT systems play a critical role in supporting FEMA to accomplish its response and recovery efforts. The OCIO supports FEMA's mission by enhancing and maintaining the IT infrastructure, increasing efficiencies and cooperation across division and region lines, and developing and enhancing key systems. FEMA has approximately 90 operational systems used to provide support across multiple programs. Although many of FEMA's systems do not solely belong to the OCIO, the OCIO partners with FEMA's program offices to provide support with systems development, testing, implementation, and operations and maintenance efforts. FEMA's primary mission critical systems are listed below.

Logistics Management Systems: FEMA's Response component uses a number of systems to support the procurement and delivery of goods and services during disasters. Key systems include the following:

- Logistics Information Management System III (LIMS III) – The agency's property/asset management system used to maintain the inventory of equipment and supplies.
- Logistics Supply Chain Management System (LSCMS) – [Previously known as Total Asset Visibility (TAV)] Provides key supply chain management capabilities for purchasing/ordering, order fulfillment, inventory maintenance, transportation, and delivery and acceptance.
- eTasker – A web-based system that field personnel use to submit requests for disaster resources such as commodities (e.g., water, ice, and meals ready to eat), to FEMA headquarters. It also coordinates information for requests that involve transportation requirements.

Response and Recovery Systems: Includes disaster and nondisaster systems implemented by FEMA's Recovery component to help the agency perform mission operations during and after a disaster.

National Emergency Management Information System (NEMIS) – The backbone system for response and recovery operations that FEMA uses to electronically enter, record, and manage information on registered applicants for disaster assistance, obligations and payments, emergency management mission assignments, and grants. NEMIS is composed of several modules:

- NEMIS Individual Assistance – Used to facilitate the application process for disaster assistance.
- NEMIS Public Assistance – A web-based application used by state and local governments to request federal assistance to repair their damaged facilities and infrastructure in national disasters as well as to track resulting project reviews, approvals, and grants.
- Emergency Management Mission Integrated Environment (EMMIE) – A single grants-processing system that serves all grants within FEMA.

Mission Support Systems: Includes systems managed within the Mission Support Component to support mission operations.

- Integrated Financial Management Information System (IFMIS) – FEMA's primary accounting general ledger, financial management, acquisition, and disbursement system. It forwards financial information to the Department of the Treasury for payment of disaster assistance claims.
- ProTrac – The contract management and tracking software used by the Acquisition Management Division of the OCIO.
- Automated Deployment Database (ADD) – Used to identify and deploy personnel to disaster sites.

Effective management of these systems is important to ensure that the technology can support disasters. In 2007, the OCIO began focusing on efforts to better stabilize and integrate these IT systems across the agency. In 2008, FEMA awarded a $1 billion contract for Enterprise Application Development Integration and Sustainment (EADIS), a range of application development services, to help create a more integrated computer environment for the operation of FEMA's systems.

Historically, FEMA's IT systems have not fully supported the agency's needs during major disasters. For example, major hurricanes during 2004 and 2005 exposed numerous limitations in FEMA's IT foundation and system capabilities to support emergency support operations. We have completed a number of audits addressing FEMA's use of IT to support mission operations:

- In a September 2005 report, we identified a number of IT management issues limiting the agency's effectiveness.[1] Specifically, we found that system improvements and additional IT user support were needed to better support response and recovery operations. Also, we reported that FEMA had not achieved alignment of its IT approach with the DHS mission and plans. We recommended that FEMA update its IT strategic plan; complete its enterprise architecture; ensure that personnel receive systems training, guidance, and communication; ensure participation in the process to develop and maintain business and system requirements; and develop and maintain a testing environment and ensure that configuration management activities are followed and documented.

[1] *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery*, OIG-05-36, September 2005.

- In December 2006, we reported that FEMA had demonstrated short-term progress by increasing system capacity and online system access, as well as developing a plan to implement training improvements along with new business and IT tools.[2] However, we found that significant challenges remained for FEMA to establish a long-term strategic IT direction and to define requirements for needed system modernization improvements. Thus, all recommendations from the 2005 report remained open and no further recommendations were issued.

- In May 2008, we reported that FEMA's IT systems did not support logistics activities effectively.[3] We recommended that FEMA finalize its logistics, strategic, and operation plans; develop, communicate, and implement processes and procedures; evaluate current IT systems to determine their ability to support operations; and develop a strategy for acquiring IT systems.

In addition, the Government Accountability Office (GAO) has reviewed FEMA's use of IT to support its mission operations. In a November 2008 report, the GAO identified actions FEMA was undertaking to implement the *Post-Katrina Act*.[4] Specifically, GAO reported that FEMA had initiatives in progress to improve information sharing and communication between systems, such as LIMS III, TAV, and ADD, by FY 2009. Also, in March 2009, the GAO reported that FEMA had developed a TAV communications plan, emphasized training for TAV, identified additional TAV specialists, and was addressing connectivity issues needed to improve operations.[5]

[2] *FEMA's Progress in Addressing Information Technology Management Weaknesses*, OIG 07-17, December 2006.
[3] *Logistics Information Systems Need to Be Strengthened at the Federal Emergency Management Agency*, OIG-08-60, May 2008.
[4] *Actions to Implement the Post-Katrina Act*, GAO-09-59R.
[5] *Actions to Implement Select Provisions of the Post-Katrina Emergency Management Reform Act*, GAO-09-433T.

Results of Audit

FEMA Needs Effective IT Planning to Guide Modernization Efforts

FEMA has a number of IT infrastructure modernization initiatives under way. However, FEMA does not have a clear end-state vision for modernization of its IT infrastructure and mission-critical systems. Specifically, FEMA does not yet have a comprehensive IT strategic plan to coordinate and prioritize modernization initiatives and IT projects. The existing plan does not include clearly defined goals and objectives, nor does it address program office IT strategic goals. In addition, FEMA has not completed its efforts to document the agency's business functions, information resources, and IT systems as part of its baseline enterprise architecture. Without these elements in place, FEMA is challenged to establish an effective approach to modernize its IT infrastructure and systems.

FEMA IT Modernization Initiatives Are Under Way

FEMA is pursuing a number of initiatives to modernize its IT infrastructure. Specifically, the OCIO has identified a number of enterprise modernization efforts to implement over the next five years, as detailed in figure 3.

Modernization Projects Under Way	Description of Intended Functions	Proposed Benefit
Transition to DHS' OneNet	Consolidate networks into DHS' OneNet.	Increase efficiency and standardization.
DHS Data Center Migration	Reduce the number of existing data centers to two secure, geographically diverse locations to enhance the department's disaster recovery capabilities. FEMA will transfer approximately 300 systems over the next five years.	Ensure that each mission-critical system has disaster recovery, redundancy, and backup capabilities. Reduce costs while streamlining maintenance and support contracts.
EADIS	Provide a full range of application services that will create an integrated environment for the operation of FEMA's programs.	Deliver secure, service-enabled applications that share mission-critical information across organizational lines.

Modernization Projects Under Way	Description of Intended Functions	Proposed Benefit
"One-One-One Program"	Promote mobility for all FEMA staff with one notebook computer, one encrypted flash drive, and one smart phone to each employee.	Improve mobility while improving data security and standardization of equipment and software across the agency.
Windows 7 Operating System	Standard baseline image for desktops will use the Windows 7 operating system.	Reduce the number of desktop images across FEMA. Windows 7 is Federal Desktop Core Configuration compliant.
Alteris Monitoring Tool	Deploy in conjunction with Windows 7 to better manage the desktop image.	Improve software patch management and license management capabilities.
Enterprise Shared Workspace / SharePoint	Provides a range of web collaboration and application capabilities.	Increase adherence to departmental standards and guidelines for intranet sites and streamline the web-hosting process.
Video Teleconference Capability	Modernize FEMA's baseline infrastructure.	Improve teleconference and video capabilities for all regions.
New Email Capabilities	Provide "email as a service" at Data Center 2.	Reduce email costs by half, increase email capacity, and add recovery, testing, and archival capabilities.
Consolidation of Software Licenses	Consolidate software licenses.	Realize a cost savings through consolidated enterprise and infrastructure software licenses.

Figure 3: OCIO's IT Infrastructure Modernization Initiatives

Some of these initiatives began as a result of departmental guidance, such as efforts associated with the transition of FEMA's networks to DHS OneNet and the DHS Data Center consolidation. Specifically, in 2003, DHS began to consolidate its components' existing infrastructures into DHS OneNet, a wide area network, for a more efficient and standardized architecture. Also, the DHS Chief Information Officer (CIO) established the "One Infrastructure" vision to improve information sharing via an enterprise-wide, consolidated data center IT infrastructure. The

objective of this initiative is to collocate and consolidate the numerous disparate data center facilities that currently support the DHS components.

Other IT infrastructure efforts were initiated in response to the FEMA Administrator's vision for more real-time, mobile technology. For example, the "One-One-One Program" is meant to increase mobile computing capabilities by providing one notebook computer, one encrypted flash drive, and one smart phone to each employee. According to the OCIO, this program will also improve data security and will help standardize equipment and software across the agency.

In addition to these IT infrastructure modernization initiatives, FEMA is taking steps to replace some of its key mission systems. For this, FEMA is working with DHS in its Transformation and Systems Consolidation (TASC) initiative, which is intended to consolidate and integrate systems essential to operations across DHS. Four business functions, including budget, finance, acquisition, and property will be included in this effort. According to OCIO leadership, this initiative will serve as a replacement or upgrade for a number of FEMA's critical systems, including IFMIS and LIMS III, which are used for finance and property functions.

FEMA governs these efforts with enterprise processes and management controls, such as program management offices, working groups, and executive steering groups and committees for decision making. For example, steering groups have been established to help guide logistics supply chain, grants management, and disaster management efforts.

Comprehensive IT Strategic Planning and Architecture Is Needed

The OCIO has not performed the necessary planning activities to guide its IT modernization efforts. Although the OCIO has a management control structure in place to govern its key modernization efforts, FEMA does not yet have a comprehensive IT strategic plan, with well-defined goals, objectives, milestones, and measures, to guide these activities. According to the *Federal Enterprise Architecture Practice Guide*, the agency should only make investments that move the agency toward the target architecture, which should also be closely aligned with the

organization's strategic plan.[6] However, FEMA does not yet have an effective IT strategic plan or a completed architecture that can be used to guide and constrain IT development and modernization efforts. Without these, the agency does not have a complete picture of its strategic IT goals or a sequential plan to prioritize modernization efforts.

IT Strategic Goals and Objectives Are Not Defined

A comprehensive IT strategic plan is key for guiding and coordinating the agency's modernization projects and IT activities. The *Government Performance and Results Act of 1993* holds federal agencies responsible for strategic planning to ensure efficient and effective operations and the use of resources to achieve mission results.[7] A strategic plan should provide guidance for program activities by including outcome-related goals and objectives and a description of how the goals and objectives will be achieved. Further, *DHS Management Directive (MD) 0007.1* requires component CIOs to develop and implement an IT strategic plan.[8] The plan should clearly define how IT supports an agency's mission and drives investment decisions, guiding the agency toward its goals and priorities.

We reported in 2005 that FEMA had not yet demonstrated effective IT strategic planning that was aligned with agency and departmental direction.[9] We recommended that FEMA update its IT strategic plan in line with the FEMA strategic plan. To address this shortfall, the OCIO completed its first official IT strategic plan, the *FEMA ITD Strategic Plan: FY 2009–2013*.

The IT strategic plan was developed to align with the *FEMA Management Directorate Strategic Plan FY 2009–2011* and the *DHS IT Strategic Plan FY 2009–2013*.[10] To that end, FEMA's IT strategic plan is meant to address how the OCIO will accomplish the goals listed in the FEMA and DHS strategic plans, as shown in figure 4.

[6] Chief Information Officers Council, *A Practical Guide to Federal Enterprise Architecture*, February 2001.
[7] Public Law 103-62, *Government Performance and Results Act of 1993*, August 3, 1993.
[8] DHS, Management Directive 0007.1, *Information Technology Integration and Management*, March 15, 2007.
[9] *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery*, OIG-05-36.
[10] FEMA, *FEMA Management Directorate FY 2009–2011*, October 2008; DHS OCIO, *DHS IT Strategic Plan FY 2009–2013*, January 2009.

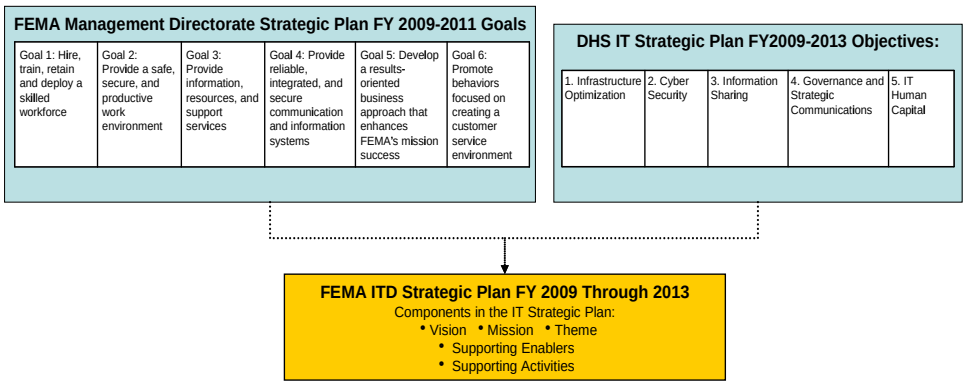

Figure 4: IT Strategic Planning Approach

FEMA's 2009–2013 IT plan includes an IT mission and theme. Specifically, the mission of the OCIO is "to enhance and maintain IT infrastructure; develop and enhance key systems to support operating programs; and increase efficiencies and cooperation across the FEMA directorate and regional lines." The plan's overarching IT theme is to "empower emergency management and preparedness." The plan also describes how the OCIO will support FEMA's six Management Directorate goals. Finally, the plan contains a high-level summary of activities, listed in an appendix, to be executed during FY 2009–2013. For example, the plan lists nearly 50 activities that were to be completed by FY 2013, such as developing and retiring numerous IT systems.

Although FEMA's IT strategic plan contains a high-level summary of the IT efforts planned, it does not provide the detailed guidance necessary for FEMA's IT program activities. Specifically, it does not include IT strategic goals or objectives to identify how IT will be used to support agency-wide programs. According to Office of Management and Budget (OMB) Circular A-130, the IT strategic plan should provide a description of how IT activities help accomplish agency missions.[11] Thus, a strategic plan should include results-oriented goals, objectives, and initiatives to specify which actions to accomplish during a given period. For example, IT goals address key areas of focus for the organization to realize the future vision, while IT objectives describe the actions needed to achieve each goal. Specific goals and objectives are critical for FEMA to ensure that effective guidance is in place to coordinate the agency's numerous ongoing modernization projects and IT activities.

[11] OMB Circular A-130, *Management of Federal Information Resources*, November 28, 2000.

IT Strategic Plan Does Not Include Program Office Initiatives

FEMA's IT strategic plan is not a comprehensive plan for the agency's IT because it primarily addresses the IT initiatives that are planned within the OCIO, and does not include numerous IT-related efforts under way across FEMA's program and regional offices.

Some program offices have developed their own IT strategic plans. For example, the Logistics Management Office developed a strategic plan in 2009, which includes a strategic goal for IT systems development.[12] According to the plan, the directorate will develop integrated logistics management systems. Four objectives were established: to develop a logistics supply chain management system, a property accountability system, an inventory management system, and a maintenance management system. Likewise, the *Grant Programs Directorate Strategic Plan FY 2009–2011* states that the directorate will bring together various grant management systems to improve data collection and analysis functions.[13] The directorate has identified two specific objectives aimed at implementing and releasing the Non-Disaster Grants System. However, the FEMA IT strategic plan does not identify the numerous efforts documented in program office strategic plans such as these to ensure that major IT initiatives are understood and managed appropriately.

Without an agency-wide IT strategy to bring together IT efforts, FEMA is hindered in its ability to define an enterprise-wide vision for modernizing IT infrastructure and systems to improve disaster response capabilities. Likewise, there is no clear guidance to emphasize which overarching technologies or programs are most critical to support the agency. As a result, IT development and operations activities are not prioritized. Instead, IT development efforts are initiated by FEMA program offices to meet program-level goals each fiscal year. For example, the Logistics Directorate had four primary IT development efforts under way for FY 2010 to support its goal to "develop integrated logistics management systems." Although the OCIO collaborates with the directorate on these IT efforts, they are not tracked or prioritized against other FEMA program efforts agency-wide.

[12] FEMA, *Logistics Management Directorate Strategic Plan FY 2010–2014*, September 2009.
[13] FEMA, *Grant Programs Directorate Strategic Plan FY 2009–2011*, October 2008.

OCIO officials said that the current IT strategic plan was developed as an effort to focus on the mission support needs within FEMA's Management Directorate. The strategic planning approach encouraged the OCIO to identify relevant issues on which to focus, such as IT system availability, integration, reporting, project management, and internal controls. However, the CIO acknowledged that the current plan does not include an overarching modernization approach. The CIO said that the agency is aware of the importance of further developing its strategic planning functions; however, there is a need to mature these capabilities first. In the meantime, the OCIO is taking steps to better understand program office needs, other customer needs, and long-term plans by partnering with its customers to document IT investment plans and participate in decision making.

In the absence of a comprehensive IT strategic plan, the OCIO and its customers will continue to focus on immediate needs, rather than addressing the long-term modernization efforts necessary to improve disaster response operations. Additionally, until FEMA develops such a plan, it faces an increased risk that the agency's IT modernization may not adequately meet its urgent mission needs.

Complete Enterprise Architecture Is Needed

According to GAO's IT Investment Management Framework, an effective IT investment management approach integrates strategic planning and enterprise architecture to ensure that IT investments directly support the fulfillment of the agency's strategic goals and objectives.[14] For example, while the IT strategic plan establishes direct linkage between agency strategic goals and its IT investments, the enterprise architecture identifies what technology is needed to support the agency, which enables alignment and prioritization of investments.

The *E-Government Act of 2002* requires that agencies develop an enterprise architecture to govern their business processes and IT.[15] However, significant work remains for FEMA to develop a complete agency-wide architecture that can be used for disciplined IT investment management decision making to guide and constrain investments and to provide a blueprint for IT modernization.

[14] *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G, March 2004.
[15] *E-Government Act of 2002*, Public Law 107-347, December 17, 2002.

Enterprise architecture is the discipline of capturing information about the organization to support strategic planning, guiding information technology investments, promoting better utilization of enterprise resources, and minimizing redundancies and waste. The OCIO has made progress toward establishing the agency's architecture and associated guidelines. Specifically, the OCIO has established a dedicated Enterprise Architecture Office (EAO) to oversee agency-wide architecture efforts. Recent efforts include plans for a comprehensive baseline agency-wide architecture, known as the FEMA Composite Architecture. According to the EAO, architecture information has been gathered and documented for some major infrastructure and systems applications, such as grants management.

The OCIO has also established agency-wide architecture policies and guidelines. In particular, the EAO has set up policies for conducting system life cycle reviews as part of the OCIO's processes to approve or deny OMB "Exhibit 300" documentation.[16] For example, the EAO participates in detailed reviews of business cases for IT solutions to ensure that system development efforts comply with DHS architecture and security guidelines. Additionally, the EAO has provided guidance on its intranet site to support OMB "Exhibit 300" architecture-related questions. The website also provides a list of technical standards and product specifications to guide agency-wide IT purchases.

Although FEMA has made significant progress, the agency has not completed efforts to document its business functions, information resources, and IT systems as part of its baseline enterprise architecture. IT architecture information remains undocumented for many program areas. In addition, the EAO stated that the life cycle review process needs to be further streamlined to reduce the number of documents required as part of the review. Further, the standards on the EAO's web site are two to three years out of date. For example, the printer and laptop specifications are dated 2007 and 2008, respectively.

The OCIO plans to complete the baseline architecture by 2012. However, these efforts have been hindered by staffing and funding shortages. The EAO's current staff of five employees falls short of

[16] Exhibit 300s are documents by which project teams can demonstrate to OMB and agency management 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.

its identified need for eight employees, plus additional contractor support. Additionally, OCIO management said that the focus in recent years, both in terms of staff and funds, has been on providing IT solutions to meet high-priority disaster response efforts, rather than on documenting its architecture. However, the OCIO awarded a contract in May 2010 to help FEMA complete its composite architecture effort.

In the absence of a completed agency-level architecture, FEMA has relied on the DHS enterprise architecture to provide technical guidelines. For example, FEMA is using the DHS Technical Reference Model to facilitate its agency-level technology request process.[17] This process is required to ensure that equipment and software requests are allowed within DHS before FEMA makes a purchase. However, the EAO said that the process is neither efficient nor effective because of the outdated technology on the DHS Technical Reference Model. According to the EAO, it takes an average of two months to process a request to obtain approval to add new technology to the model.

Without a comprehensive baseline architecture, the OCIO is hindered in guiding IT investments toward a standardized and integrated environment. The OCIO is further challenged by the lack of a detailed IT strategic plan, which is needed to ensure that the enterprise architecture is aligned with the organization's IT strategic goals. Without these elements in place, IT investment decisions are made without clear rationale or prioritization, which may lead to IT systems that do not meet the agency's long-term needs. Consequently, systems will continue to be created in an independent and nonintegrated manner, resulting in an IT environment with predominantly stand-alone functionality and an inability to share data across systems.

[17] The Technical Reference Model is a technical framework that categorizes the standards and technologies to support and enable the delivery of service components and capabilities.

IT Needs Throughout FEMA Are Not Well Understood

The OCIO does not yet have a good understanding of existing IT resources and needs throughout FEMA. Specifically, FEMA does not have a complete inventory of its systems to support disasters. Although the OCIO has sought to establish a complete systems inventory, these efforts have been hindered by multiple independent inventories that are not shared across the organization. In addition, FEMA program and field offices continue to develop IT systems independent of the OCIO because of the way funds are managed for IT efforts. Furthermore, although the OCIO established a standard IT development approach, FEMA has been slow to adopt this process. IT systems developed without the oversight and guidance of the OCIO may not provide the support needed to coordinate activities effectively during major disasters.

IT Systems Inventory Is Not Complete

According to the *Clinger-Cohen Act*, the CIO is responsible for developing, maintaining, and facilitating the implementation of an integrated IT architecture, as well as promoting the effective and efficient design and operation of all IT resources.[18] Further, according to *DHS MD 0007.1*, each DHS component CIO is responsible for the effective management and administration of all IT resources and assets to meet mission, department, and enterprise program goals.

The effective management of agency-wide IT resources and assets requires a complete and accurate inventory of systems. However, the OCIO does not maintain a comprehensive list of all FEMA program office and regional systems. Although the OCIO has established an official systems inventory of approximately 90 operational systems, OCIO officials estimate that several hundred "rogue" systems at FEMA regions are not yet captured on this inventory.

Numerous separate inventories are maintained throughout the agency, which hinders the OCIO's ability to establish a complete and accurate inventory of all FEMA systems. For example, the Logistics Directorate maintains its systems inventory in its Logistics Systems Group. The Recovery Office maintains an inventory of IT systems and tools within the IT branch of its program office. OCIO personnel estimate that the number of

[18] Public Law 104-106, February 10, 1996.

FEMA's systems across all regional offices ranges from 90 to as high as 700.

The OCIO recognizes the need to improve outreach efforts to IT users and has established a number of methods to increase awareness of the systems developed by program offices and regional offices. For example, the OCIO has assigned each program office a customer advocate. Customer advocates act as liaisons between OCIO and program office IT personnel to increase understanding of the IT systems in use and increase partnership in IT efforts. The OCIO also uses methods such as data calls to inquire about the systems in use. As additional systems are discovered on FEMA's network, the OCIO documents each system and issues an authority to operate until proper security protocol can be completed.

The OCIO is also creating a "scorecard" for each program office to document all of the agency's systems. The scorecard includes the development and maintenance schedule and funding for each system. For example, the Recovery Office scorecard includes 16 operational systems. Although these efforts have helped the OCIO establish better visibility of IT systems, significant work remains for the OCIO to establish a complete, comprehensive list of all systems in use across FEMA.

Program and Regional Offices Fund and Develop Their Own IT Systems

The way IT programs are funded and developed within FEMA has hindered the OCIO's efforts to establish a complete inventory and manage IT capital planning and investment. Specifically, IT development efforts are conducted throughout FEMA's regional and program offices. Although the OCIO has developed a standard systems life cycle practice to be used for all IT projects, the process has not yet been institutionalized throughout FEMA.

FEMA Program Offices Receive Direct Funding to Develop IT Systems

The DHS CIO has responsibility for IT policy and programs, such as IT capital planning and investment management functions.[19] Additionally, according to *DHS MD 0007.1,* each DHS component

[19] *Information Technology Management and Governance Processes Catalog,* Department of Homeland Security, Office of the Chief Information Officer, July 2009.

CIO is responsible for preparing an IT budget that includes all of the component's IT activities.

OCIO officials said that the decentralization of IT funds and development has been a major obstacle to effective management of the IT environment. During FY 2010, FEMA spent $391 million for agency-wide IT needs. OCIO IT spending of $113 million accounted for only 29% of total spending. The program offices spent approximately $278 million, which comprised the majority of the agency's IT-related spending, as shown in figure 5.

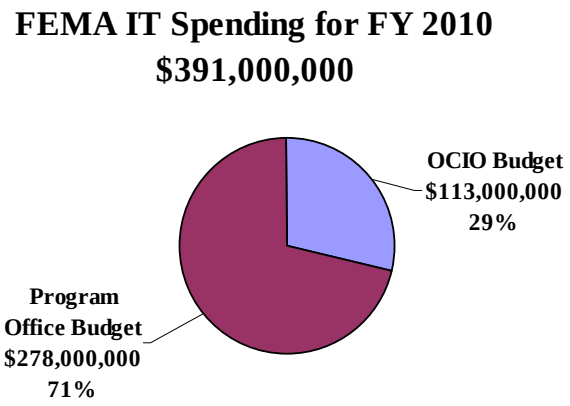

Figure 5: FEMA IT Spending for FY 2010

FEMA's program offices receive funds for operations, maintenance, and administration each fiscal year, including funds that they use for independent IT efforts. For example, the Recovery Office managed an IT budget of approximately $44 million in FY 2010; the Logistics and Management Division, $33 million; and the Mitigation Office, $34 million. Because they receive direct funding for IT and do not have to rely on IT support from the OCIO, program offices have historically developed IT systems without input or guidance from the OCIO.

Deploying new systems on the network without prior OCIO involvement creates concern as to whether the systems will operate in the existing environment, meet security standards, or contain redundant IT elements. For example, one FEMA directorate attempted to develop an IT system without the involvement of the OCIO. The directorate spent approximately $7.5 million on the system, which ultimately was unable to meet FEMA's security and technical requirements. In another case, a regional office created a Microsoft Access database to address the data-sharing limitations between IFMIS and ProTrac. This tool was developed to help

synchronize the data and produce timely reports. Since its creation, the database has been shared across multiple regions. To the extent that such systems are networked, they pose potential risks to infrastructure operations.

The OCIO has taken steps over the past two years to establish policies and guidance for IT programs. Specifically, the OCIO has been working to establish a process to streamline reviews of IT spending. Accordingly, the CIO issued agency-wide guidance in 2008 requiring review and approval of all IT spending over $10,000. FEMA's Office of Procurements is responsible for forwarding IT acquisition requests over $10,000 to the CIO for review. However, without a more formal control mechanism in place, FEMA programs are reluctant to comply with this process.

Systems Life Cycle Process Has Not Been Institutionalized

To comply with the DHS policy and procedural guidance for IT management, the OCIO adopted a standard systems life cycle process in 2008 for all IT projects. This process is based on the DHS System Engineering Life Cycle (SELC) approach. The OCIO is using its application development contract, EADIS, to implement the process and to ensure that standardized practices are followed in IT development efforts. Figure 6 shows the SELC stages.

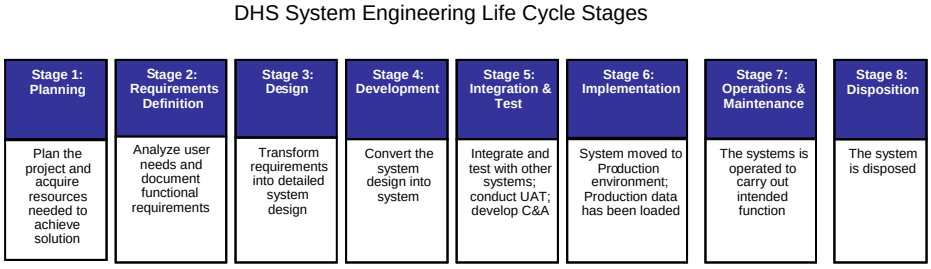

Figure 6: DHS SELC Stages

In 2008, the OCIO directed all FEMA organizations to use the SELC process for IT projects. Since that time, FEMA has steadily increased the number of IT projects using this approach. As of July 2010, approximately 35 projects were being managed within the EADIS structure. However, these projects do not account for all IT development work currently under way across FEMA.

The OCIO stated that FEMA program offices have been reluctant to employ the SELC approach due to increases in the costs for EADIS support. IT development support using this approach has

higher costs than similar OCIO services provided in the past. This is due to the fees associated with EADIS contract services, such as the use of dedicated production and hosting environments. Consequently, numerous program offices told us that IT project costs have increased by approximately 50% since using EADIS support. One program office faced an increase from $2.7 million to $6.4 million to gather requirements and develop the web-enabling capability for the NEMIS system.

Concerns over the additional time spent to complete IT development steps required for the SELC process have also prevented some program offices from using this process. One program office said that it prefers its "rapid development approach" for IT development, which allows for quicker deployment for the new tools needed to support mission efforts. However, this approach does not comply with departmental IT development standards associated with the SELC, such as documenting requirements and conducting testing.

Because of such concerns, some program offices continue to use their own IT development methodologies. For example, one program office has built applications using its "rapid development approach." According to personnel in this office, information-sharing and reporting tools have been developed using this approach.

IT systems developed using methodologies outside of the SELC and without OCIO involvement may not align with mission, department, and enterprise program goals. The systems may not meet department-wide requirements, may create potential security risks, or may duplicate other efforts. More important, such systems may not provide the support needed to coordinate activities effectively during major disasters.

IT Infrastructure Improvements Have Been Made, But Further Improvements Are on Hold

The OCIO has completed a number of improvements to enhance its IT infrastructure foundation and disaster response system capabilities. However, efforts to modernize some of the agency's critical mission support systems have been put on hold due to department-wide consolidation plans and the reduction of funding for these systems. As a result, the legacy systems do not provide the functionality needed to support FEMA's disaster response mission operations in a timely and effective manner.

IT Improvements Have Been Made

FEMA has completed a number of improvements to its IT infrastructure and systems. For example, the OCIO has taken steps to improve its IT infrastructure foundation by strengthening security, improving the IT development environment, increasing network bandwidth and connectivity, and updating the infrastructure supporting response and recovery IT capabilities. FEMA has also improved its disaster response system capabilities.

Infrastructure Improvements

To improve desktop computing capabilities and security, the OCIO established an agency-wide desktop image, which was deployed to FEMA computers in FY 2009. FEMA has improved its email capabilities by increasing capacity and adding recovery, testing, and archival capabilities, thus reducing email costs. The OCIO has improved its telephone services by adding text messaging, global positioning capabilities, and data services. Additionally, the OCIO has centralized the management and provisioning of services for its video teleconferencing capability and upgraded the hardware and management processes. The OCIO has also reduced high-risk vulnerabilities on its network and increased efforts to ensure that all new applications receive official authority-to-operate certificates before being placed on FEMA's network. Finally, the OCIO has improved FEMA's security posture by maintaining a *Federal Information Security Management Act* score above 90%.[20] This achievement surpassed the OCIO's initial target of 90% for FY 2009, as identified in its *IT Strategic Plan FY 2009–2013*.

[20] DHS FISMA, *Fiscal Year 2009 FISMA Report and Privacy Management Report*, November 2009.

The OCIO has also improved the IT development process by establishing a dedicated testing environment to ensure that configuration management activities are followed and documented during IT development efforts. Specifically, two new complete testing environments were put into operation in FY 2009, which represent approximately 50 FEMA systems. This improvement also addresses recommendations made in our 2005 report to develop and maintain a testing environment that ensures that all systems components are properly and thoroughly tested.[21]

Furthermore, the OCIO has taken steps to improve its network bandwidth and connectivity. For example, FEMA is participating in a department-wide effort to consolidate its IT infrastructure into DHS OneNet, a wide area network. As of June 2010, the OCIO had completed the transition of all network connections at its regional sites to DHS OneNet. According to the OCIO, this has improved network throughput and increased security, enabling FEMA personnel to share information more securely across a common DHS network platform.

FEMA has also made progress in updating the infrastructure supporting response and recovery IT capabilities. For example, the OCIO completed a consolidation of NEMIS servers in June 2010. This effort reduced the number of servers, previously located at all ten regional offices, to three, resulting in increased system availability, improved network performance, and better system security.

System Improvements

FEMA has replaced its TAV system with LSCMS. This effort replaced paper-based processes and a multitude of outdated disaster property and commodities management systems, providing updated information for timely decision making.

FEMA also enhanced the NEMIS Public Assistance module by adding the EMMIE web application in 2007. This web-based module is currently used by the Public Assistance program to manage grants for disasters and will be expanded to the Mitigation program. The EMMIE module benefits FEMA personnel by providing better authentication, authorization, and accessibility.

[21] *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery,* OIG-05-36.

Additionally, FEMA enhanced the NEMIS Individual Assistance module as follows:

- NEMIS registration intake functions were put online using a web-based capability called the Disaster Assistance Improvement Program. This program provides a single, online access point for individuals requiring assistance, and also provides online registration and status-tracking capabilities.
- The Direct Assistance Replacement Assistance Consideration system replaced the FEMA Response and Recovery Applicant Tracking System in 2007, resulting in a consolidation of 50 Microsoft Access databases. The Direct Assistance system can automatically populate data, such as the applicant's address, once key information is entered in the system, resulting in a reduction of handling time per call.
- The Document Management and Records Tracking System replaced the ViewStar system to read and process incoming mail from applicants. The implementation of the document management system increased security as well as the speed of data and image retrieval, resulting in saved time.

Further System Improvements Are on Hold

The OCIO identified the need to modernize IT assets onto a common, stable platform and to integrate its mission-critical systems as part of its 2007 "critical imperatives." Although FEMA has improved its IT infrastructure and its disaster response system, significant work remains for FEMA to complete the system modernization upgrades that are needed to integrate the agency's critical mission support systems and improve their functionality.

FEMA has been challenged to modernize its systems in order to achieve integration due to plans for a department-wide integrated asset management, financial, and acquisition solution. Specifically, FEMA personnel are working with DHS officials on the TASC initiative to achieve a department-wide integrated asset management, financial, and acquisition solution. This initiative will provide enterprise applications that will likely replace the LIMS III, IFMIS, and ProTrac systems by 2014. Although FEMA is scheduled to be the first to receive the new TASC solution, the department has not yet confirmed the dates when each system will be replaced. Additionally, the department's detailed plans, such as the selection of new applications, are not known. In the meantime, FEMA is not able to plan or fund system upgrades, which are

needed to ensure that IT can support FEMA's disaster response mission operations in a timely and effective manner.

Funding has been reduced for the systems that will be replaced as part of the DHS TASC initiative. Specifically, funding to support LIMS III has fallen over the past three years. For example, annual funding to support development, operations, and maintenance for LIMS III prior to 2008 was approximately $1 million. However, funding was reduced to about $420,000 in FY 2010. Consequently, LIMS III has received only minor enhancements during that time. FEMA has expended minimal resources for system operations and maintenance to provide the basic property management functions needed. An OCIO official said that FEMA's goal is to sustain the system until the transition to the department's TASC solution.

Likewise, funding to improve IFMIS reporting capabilities and achieve integration with FEMA's acquisition functions has been limited. An OCIO official said that, although IFMIS has been kept as up-to-date as possible with modifications and enhancements, a major overhaul or system replacement is necessary to meet surging high-volume disaster support requirements. However, the agency is unable to perform significant enhancements because of decreased funding for IFMIS development efforts. For example, the Office of the Chief Financial Officer received $5.34 million for program support in FY 2009; however, this was reduced to $4.85 million in FY 2011. FEMA is also constrained by the increasing cost of the IFMIS software updates, which are expensive because of its 20-year-old technology. Consequently, FEMA was instructed to refrain from major system upgrades or additional development until the DHS TASC solution is implemented.

FEMA Technology Does Not Effectively Support Operations

Federal regulations require that agencies plan in an integrated manner for managing IT throughout its life cycle. Specifically, according to *DHS MD 0007.1*, the component CIO shares accountability with the Under Secretary for Management for successful planning and implementation of functional integration. Furthermore, according to the *Clinger-Cohen Act of 1996*, the CIO is responsible for developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency.

FEMA's IT application environment has evolved to include a number of legacy mission systems that do not effectively meet user

requirements. Specifically, FEMA's mission-critical systems are not integrated, and FEMA personnel must still perform some tasks manually.

Critical Systems Are Not Integrated

The OCIO said that integration is needed across a number of FEMA's essential operational functions, including asset management, financial management, and acquisitions. However, FEMA's mission-critical systems, such as LIMS III, LSCMS, ADD, IFMIS, and ProTrac, operate with predominantly stand-alone functionality and cannot perform integrated functions.

For example, FEMA has not integrated the systems used in its property inventory and supply chain processes. In 2008, we reported that FEMA did not have a comprehensive system to account for its commodities and provide real-time awareness.[22] FEMA is still challenged by the fragmentation of data across multiple logistics systems. Specifically, the property management system, LIMS III, and the supply chain management system, LSCMS, are not integrated. Most commodities, such as IT equipment and furniture, are tracked in both systems, with staff performing the same functions in each system. Because inventory and tracking data do not automatically feed from LSCMS into LIMS III, users must manually enter data in LIMS III to close out an order. Consequently, the processes for shipping and receiving are labor-intensive and redundant. Also, the information in LIMS III is not timely or accurate because data are not automatically shared between LIMS III and LSCMS as commodities are shipped. For example, when trucks are dispatched from a supplier, the shipment does not show up in LIMS III until FEMA personnel receive the shipment. Personnel must manually update LIMS III as shipments are received. Until this step is completed, data in LIMS III will not reflect recently received shipments.

Similarly, FEMA has not integrated systems to support personnel and property management functions. We previously reported that FEMA's personnel deployment system, ADD, and its property management system, LIMS III, did not support effective or efficient coordination of deployment operations.[23] FEMA

[22] *Logistics Information Systems Need to Be Strengthened at the Federal Emergency Management Agency*, OIG-08-60.
[23] *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery*, OIG-05-36; *Logistics Information Systems Need to Be Strengthened at the Federal Emergency Management Agency*, OIG-08-60.

employees must still complete a number of steps to manually check in and obtain property, such as IT equipment, at a disaster site. Although FEMA has made minor improvements to each system, the agency has not yet implemented an interface between ADD and LIMS III, and there are no plans to develop an interface at this time. Until an effective link between the personnel and property management systems is established, FEMA faces additional work and potential losses due to inefficient management of property and personnel.

FEMA's ability to track and manage disaster-related funds is hindered by the fact that IFMIS, the financial system, and ProTrac, the acquisitions system, are not integrated. Combined, these systems handle 80% of budget disaster funds. However, each system operates on a different technical platform, with financial data updates sent to each system at different times. As a result, the two systems are operating without synchronized data, and field office employees must manually track and reconcile funds that are allocated across different disaster activities. Additionally, manual steps are required to deobligate excess funds after requisitions are completed. This step should be done automatically; however, personnel performed manual deobligations that totaled $21 million for FY 2010 disaster funds.

Limited Integration With FEMA's Stakeholders

Integration with external disaster response stakeholders and partners has not yet been achieved. Integration between FEMA and its partners is critical in order to improve timely mission operations during disaster situations. This is particularly important as FEMA is the national "coordinator" during emergencies.

FEMA's IT systems are not able to integrate with its stakeholders' systems. For example, FEMA does not have an electronic capability for states to use when requesting assistance during disasters. Instead, to request federal assistance from FEMA, states use a paper Action Request Form. After the form is faxed, FEMA personnel enter request information into a tracking system that is intended to track the request through disposition. FEMA officials said that most states are now using web-enabled systems that provide capabilities for automated requests and real-time information sharing during disasters. Accordingly, the Response Directorate is planning to implement an electronic processing capability for Action Request Forms in FY 2011.

FEMA must improve its ability to work with its external partners, such as the Defense Logistics Agency, United States Army Corps of Engineers, and General Services Administration, to improve real-time sharing of assets and commodities tracking. To address this need, FEMA is currently working with its external partners to identify system interfaces between its LSCMS systems and external logistics systems to automate the order-to-receipt process. In addition, FEMA has made progress in other areas, such as its web-based EMMIE system, to allow state and local applicants to electronically apply for and track funds. However, until FEMA achieves electronic integration with its partners, they will be unable to achieve real-time total asset visibility and disaster funds tracking.

Inefficient Manual Processes Remain

In addition to the lack of integration, some systems do not provide needed automatic functions. For example, a number of functions must be completed manually outside of NEMIS. Although NEMIS eGrants is supposed to be an electronic system of records, it does not have a closeout module. Without a closeout capability, FEMA personnel must rely on paper forms and manual data entry to finalize grants in the system. During 2010, FEMA was unable to conduct electronic closeouts for approximately 187 Pre-Disaster Mitigation Grants. Additionally, officials in the Mitigation Directorate said that they must rely on a paper-based application process for the Hazard Mitigation Grant Program. Although NEMIS eGrants is used to process grants, applications are prepared and submitted on paper forms. As a result, according to FEMA's Mitigation office, an average of 100 to 200 paper applications are received during each disaster, which must be manually entered into the system.

In the absence of up-to-date IT capabilities, users must rely on systems that do not effectively meet their requirements, resulting in the need to modify processes or resort to manual work-arounds. These manual work-arounds, or informal processes, may suffice during minor events; however, they may not sustain the increased workload and level of information sharing required to support major disasters.

Conclusion

Although FEMA has begun a number of necessary modernization efforts, the OCIO has not yet completed effective IT planning activities, such as establishing an IT strategic plan or a baseline enterprise architecture. The development of an IT strategic plan that includes clearly defined agency-wide goals and objectives and the completion of FEMA's enterprise architecture are necessary to guide and constrain IT development and modernization efforts. Such plans are necessary for the agency to effectively coordinate IT projects and activities across its program and regional offices to ensure that IT investments are supporting FEMA's mission.

The OCIO is gaining a better understanding of its customers' IT needs. Recent efforts to establish an official systems inventory are an important step toward consolidating the numerous system inventories that are currently maintained across the organization. However, FEMA's program offices and regional offices continue to develop IT systems independent of the OCIO due in part to decentralized IT budget and acquisition practices. The OCIO has sought to provide agency-wide guidance for IT development efforts by establishing a standard IT life cycle approach. Yet progress in implementing this approach, as part of its enterprise application development support contract, has been slow, owing to increasing costs and the time required to complete IT development as part of the new process.

Since our last audit in 2008, FEMA has completed a number of IT infrastructure upgrades to improve security, desktop standards, network bandwidth, and the IT development environment. The agency has also completed system enhancements to provide new disaster response capabilities, such as an online registration web site. However, limited progress has been made in modernizing the agency's critical mission support systems. Such efforts have been on hold until department-wide consolidation plans are further established. As a result, FEMA's legacy systems are not able to effectively support disaster response functions in a timely and effective manner.

Recommendations

We recommend that the Chief Information Officer, FEMA:

Recommendation #1: Develop a comprehensive IT strategic plan with clearly defined goals and objectives to support program IT initiatives.

Recommendation #2: Complete and implement a FEMA enterprise architecture to establish technical standards and guidelines for systems acquisitions and investment decisions.

Recommendation #3: Establish and maintain a complete, comprehensive enterprise IT systems inventory.

Recommendation #4: Establish an agency-wide IT budget planning process to include all FEMA program technology initiatives and requirements.

Recommendation #5: Obtain agency-wide IT investment review authority to ensure that all IT initiatives and systems development efforts align with FEMA's mission.

Recommendation #6: Establish a consolidated modernization approach for FEMA's mission-critical IT systems, to include DHS plans for integrated asset management, financial, and acquisition solutions.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Chief Information Officer for FEMA. We have included a copy of the comments in their entirety in Appendix B.

In the comments, the FEMA Chief Information Officer concurred with our recommendations in general; however, the Chief Information Officer also expressed concern that the report does not sufficiently acknowledge IT modernization improvements made since 2008 and does not include sufficient measurable criteria to evaluate progress made. The Chief Information Officer provided comments on specific areas within the report to address these concerns. We have reviewed management's comments and made changes to the report as appropriate. The following is an evaluation of the issues raised, as outlined in the comments provided by FEMA.

In the comments, the FEMA Chief Information Officer expressed concern over the exclusion of progress made by the organization since 2008. Specifically, the Chief Information Officer provided an overview of FEMA's efforts to modernize its infrastructure, services, and systems. The overview includes a number of specific enterprise, business, and mission-related modernization initiatives as well as FEMA's measure of economy, efficiency, and effectiveness for each. We are aware of these efforts underway at FEMA. We have modified the report as appropriate to include additional enterprise, business, and mission-related modernization efforts. In addition, we have included FEMA's approach for managing IT modernization efforts with enterprise processes and program management structures.

The FEMA Chief Information Officer also expressed concern with the audit report methodology used to measure progress and risk, using categories such as "economy, efficiency, and effectiveness." Specifically, the FEMA Chief Information Officer stated that the current IT Strategic Plan and Enterprise Architecture provide adequate guidance for modernization efforts. However, we do not agree that FEMA's current management controls are adequate to guide and constrain IT development and modernization efforts. As part of our audit methodology, we applied specific departmental criteria with which each component is required to comply in regard to IT Strategic Planning and Enterprise Architecture, such as DHS Management Directive 0007.1, *E-Government Act of 2002*,

Clinger-Cohen Act of 1996, and *Government Performance and Results Act of 1993*.

Finally, the FEMA Chief Information Officer expressed concern with the report findings for technology that does not effectively support operations, and stated that system requirements and processes should be validated to reflect FEMA's current integration needs. However, we believe that the lack of integration causes ineffective workflow. Additionally, during our meeting with the FEMA Chief Information Officer, she expressed the importance of integrating FEMA's mission systems. Furthermore, personnel in the field stressed the need to integrate systems to improve workflow.

Report Recommendations

The FEMA Chief Information Officer agreed with the recommendations in general, however, also proposed editorial changes to the wording of the recommendations.

In response to recommendations 1–3, the Chief Information Officer proposed that the wording of the recommendations be changed to combine recommendations 1, 2, and 3. We acknowledge FEMA's rationale to focus on IT strategy and its plans to define strategic goals that can be linked to modernization activities. However, we do not agree with combining these recommendations, as doing so would make it difficult to measure progress. We will keep the recommendations as they are to individually track corrective actions taken by management to resolve each recommendation.

In response to recommendations 4–6, the Chief Information Officer proposed that the wording of the recommendations be changed to combine recommendations 4, 5, and 6. We acknowledge FEMA's efforts to integrate agency-wide program planning and activities, as well as its plans to ensure that IT investments support agency mission goals. However, we do not agree with combining these recommendations, as doing so would make it difficult to measure progress. We will keep the recommendations as they are to individually track corrective actions taken by management to resolve each recommendation.

We conducted an audit to determine whether FEMA's IT modernization approach adequately addresses planning, implementation, and management to support efficient and effective disaster relief assistance.

We researched and reviewed federal laws and executive guidance related to FEMA's support of IT systems, IT management, and CIO governance. We obtained 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. We used this information to establish a data collection approach that consisted of focused interviews, documentation analysis, and system demonstrations to accomplish our audit objectives.

We held interviews at FEMA headquarters and regional offices. We also conducted teleconferences with FEMA officials at field offices throughout the United States. Collectively, we interviewed more than 60 FEMA headquarters officials, field management officials, and system users to learn about FEMA's IT functions, processes, and capabilities. At headquarters, we met with FEMA OCIO officials including the CIO, deputy CIOs, branch chiefs, program managers, and delivery managers to discuss their roles and responsibilities related to FEMA IT management and IT infrastructure modernization. At the regional offices, we met with a division director, IT branch chiefs, IT specialists, program area specialists, system specialists, and system users to understand IT development practices, user requirements, and system use 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 FEMA's IT structure, IT management functions, current initiatives, and future plans for modernization.

We conducted audit fieldwork from July to October 2010 at FEMA headquarters in Washington, DC; FEMA regional offices in Denton, Texas, and Atlanta, Georgia; a National Processing Service Center in Denton, Texas; and a long-term recovery office in New Orleans, Louisiana. 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 Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20472

FEMA

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

FROM: Jean A. Etzel
Chief Information Officer
Federal Emergency Management Agency

SUBJECT: Comments to Draft Inspector General (IG) Report, "Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology" – *For Official Use Only, OIG Project No. 10-141-ITA-FEMA*

Thank you for giving us the opportunity to address our concerns with the Draft Inspector General (IG) Report, "Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology." We offer our comments in the spirit of continuing to enhance the economic and efficient use of Information Technology (IT) within the Federal Emergency Management Agency (FEMA), implementing the effective management of the same, and at the same time providing important critical feedback concerning the report itself and the process that led to its creation. In general, the Office of Chief Information Officer (OCIO) agrees with the recommendations the IG makes. All organizations should plan (Recommendation #1), have in place the foundational documentation for analysis and decision making (Recommendations #2 and 3), and establish processes by which to make those decisions (Recommendations #4, 5 and 6). In any well-run IT organization, the three items that form the foundation for the recommendations—planning, foundational documentation, established processes—are subject to evaluation on a continual basis with the intent of making enhancements and improvements to keep ahead of changes in the technological environment.

The OCIO, however, disagrees with the manner in which the narrative characterizes the present state of affairs at FEMA, primarily because it downplays or ignores the substantive and quantifiable progress that the organization has made since the IG's last visit in 2008. Over the past three years FEMA has undertaken important initiatives and made great progress in modernizing IT infrastructure, services, and systems. These initiatives fall into three major functional areas: enterprise, business, and mission.[1] In FEMA's IT management framework, each of the three major functional areas has categories.

[1] The enterprise functional area includes: e-Mail, Telephone (wireless, wireline, and satellite), Network (communications and security), Computing (processing, storage, web), End-User Standards, Collaboration (operational and data), Analysis and Reporting, and Service Management. The business functional area includes: Budget, Finance,

www.fema.gov

Appendix B
Management Comments to the Draft Report

In the enterprise functional area, for example, FEMA has undertaken substantive modernization efforts in 7 of 8 categories. The results of these efforts are measurable improvements in economy, efficiency, and effectiveness. One category, Analysis and Reporting, remains a work in progress, but has seen improvements in its own right. The table below summarizes some of the more significant improvements:

Enterprise Modernization Effort	Measures	Examples	Impact
e-mail	Economy	Mailbox costs reduced from about $170 to about $84 per year.	High
	Efficiency	Streamlines provisioning, billing, and closeout processes. FEMA is lead user for Department. Service managed at DC2.	
	Effectiveness	Adds larger mailboxes, testing environment, automated archiving and retrieval, and disaster recovery capabilities; designed to scale rapidly when needed.	
Telephone	Economy	Reduced overall costs by approximately $9M.	High
	Efficiency	Centralized management of service. Reduced contracting actions from 600 per year to an average of 12.	
	Effectiveness	Added text messaging, GPS, and data services. Added back-up circuits and signal amplification to FEMA locations.	
Collaboration	Economy	Obtained SharePoint per user rates of approximately $48 per user per year.	High
	Efficiency	Streamlines provisioning and hosting processes for organizational webpages. FEMA is lead user and implementing with the Department. Service managed at DC2.	
	Effectiveness	SharePoint solution offers full range of capabilities, including web pages, collaboration sites, and ".net" based applications. Office Communications Server—Provides video chat for impromptu meetings from work station to work station.	
VTC	Economy	New	High
	Efficiency	Centralized management and provisioning of services.	
	Effectiveness	Upgraded hardware and management processes increased number of possible connections from 152 to 480.	
Analysis and Reporting (Enterprise Data Warehouse)	Economy	TBD	*Low (In Progress)*
	Efficiency	Data warehouse and operational data store placed under management controls in the enterprise software development contract to eliminate duplicative processes.	
	Effectiveness	***Developing concept of operations and business case to support operations and sustainment in the future.***	
Network (OneNet)	Economy	OneNet overall costs slightly higher.	High
	Efficiency	Integrated management with the Department's network and security operations centers.	
	Effectiveness	Diversity of lines going into all fixed sites ensures continuity in the event of an outage. Increased throughput. Access protected by Trusted Internet Connections.	
Computing	Economy	Reduces hardware "footprint" at DC2—systems no longer required to have separate hardware. Cost savings TBD.	High
	Efficiency	Streamlines provisioning and hosting processes. FEMA is lead user for Department. Service managed at DC2.	
	Effectiveness	Provides integrated target "environment" for FEMA's applications. Target is rapidly scalable and resilient.	

Acquisition, Property, Human Capital, Executive Correspondence Management, and Learning Management. The mission functional area includes: Incident Management, Risk Management, Grants Management, Disaster Property and Commodities Management, Preparedness (lessons learned and exercise management), Alerts and Warning, and Emergency Communications.

2

Appendix B
Management Comments to the Draft Report

Enterprise Modernization Effort	Measures	Examples	Impact
IT Service Management (Remedy and Altiris)	Economy	Remedy Final TBD: enterprise-wide implementation reduces cost of help desk or trouble ticketing. Altiris TBD: will reduce costs for licenses and number of employees performing patching.	Medium (In Progress)
	Efficiency	Remedy: Consolidates helpdesks to the Enterprise Service Desk. Eliminated 13 so far. 6 more scheduled for FY 11. Altiris: Consolidates patch management and frees up resources in the Regions who would otherwise be doing the patching.	
	Effectiveness	Remedy: provides enterprise-wide help desk management, analysis, and reporting. Altiris: provides capability to manage licenses actively, and to manage image and security patching.	

In the business functional area, 6 of 7 categories have a solid foundation in and strong integration with the Department's efforts. Four of the categories, Budget, Finance, Acquisition, and Property, are part of the Department's Transformation and System Consolidation (TASC) effort, the business case for which has shown projections for improvements in economy, efficiency, and effectiveness. One category, Learning Management, is under analysis presently by its proponent, with the assistance of the OCIO, to plan for its modernization.[2]

Business Modernization Effort	Measures	Examples	Impact
USA Staffing (Human Capital (HC)	Economy	New	Medium
	Efficiency	Eliminated manual process. Fits within DHS's larger HC framework.	
	Effectiveness	In FY10 reduced time to recruit and fill positions from 9 to 2 months.	
RMOnline (Budget)	Economy	New	High
	Efficiency	Eliminated manual process. RMOnline part of Transformation and Systems Consolidation (TASC) solution.	
	Effectiveness	Provides budget formulation and execution capability FEMA never had before.	
IFMIS (Finance)	Economy	Reduced O&M cost from $5.5M to $2.5M. Future economies TBD—TASC business case anticipates economies.	High
	Efficiency	Consolidated from two systems (G&T and Core) to one.	
	Effectiveness	Added robust disaster recovery capability.	
LIMS (Property)	Economy	TBD—TASC business case anticipates economies.	*Low (In Progress)*
	Efficiency	Replacement (TASC) provides integrated Department-wide solution.	
	Effectiveness	Moving to DC2 to reduce hosting and hardware costs.	
Learning Management	Economy	TBD – but expected to yield economies based on consolidation.	*Low (In Progress)*
	Efficiency	Project underway to consolidate learning management systems. The project was chartered in 8/9 and the estimated date of completion is 1 to 1 ½ years from the date of contract award. Business case analysis expected to be completed 5/11.	
	Effectiveness	Present system on upgraded hardware. Test environment implemented.	
NetIQ (Executive Correspondence)	Economy	Low cost ($800 per license) Department-wide solution.	High
	Efficiency	Integrates with DHS solution. Leverages DHS contract.	
	Effectiveness	Improves functionality over previous system.	

[2] In January 2011, during the inaugural FEMAStat session, the Associate Administrator for Preparedness identified the need to put a plan in place "to guide and constrain IT development and modernization efforts" with regard to Learning Management Systems.

Appendix B
Management Comments to the Draft Report

Business Modernization Effort	Measures	Examples	Impact
Automated Purchase Requisitions	Economy	New	Medium (In Progress)
	Efficiency	Eliminates paper-based transactions. Streamlines multiple business processes used across different program offices.	
	Effectiveness	Improves tracking, accountability, and reporting capabilities.	

The mission functional area remains the most dynamic but has also seen significant improvements in economy, efficiency, and effectiveness. In the Disaster Property and Commodities Management category, in December 2010 for example, FEMA implemented a modern system (Logistics Supply Chain Management System) to achieve economy, efficiency, and effectiveness. As another example, the IT-based components of FEMA's RiskMap, a project in the Risk Management category, have transitioned to the Department's Data Center #2 to achieve significant economy, efficiency, and effectiveness.

Mission Modernization Effort	Measures	Examples	Impact
Non-Disaster Grants (ND Grants System)	Economy	***TBD***	***Low (In Progress)***
	Efficiency	Will consolidate all non-disaster grants onto one system.	
	Effectiveness	Will improve tracking, accountability, and reporting capabilities.	
Risk Management (RiskMap and National Flood Insurance Program)	Economy	RiskMap: Move to DC2 reduces costs $500K per month. Expected savings in FY12 are $3.7M. ***NFIP: TBD***	RiskMap: High ***NFIP: Low (In Progress)***
	Efficiency	RiskMap: Consolidated major infrastructure components to DC2. ***NFIP: Terminated NextGen system.***	
	Effectiveness	RiskMap: updates infrastructure and provides improved disaster recovery capability. ***NFIP: Development of new system placed under direct CIO management controls.***	
Disaster Property and Commodities (LSCMS)	Economy	New—Replaced Total Asset Visibility	High
	Efficiency	Replaces paper based and multitude of outdated disaster property and commodities management systems.	
	Effectiveness	Provides updated information for timely decision making.	
Preparedness (IPAWS)	Economy	***TBD***	***Low (In Progress)***
	Efficiency	Will share services platform with DAIP.	
	Effectiveness	***TBD***	
Incident Management (DMSE)	Economy	TBD: Pilot and proof of concept underway.	*TBD: initial capabilities will be tested during NLE-11.*
	Efficiency	TBD: Will consolidate data feeds from multiple independent systems.	
	Effectiveness	New	
Disaster Grants (Individual Assistance (IA) and Public Assistance (PA) Grants)	Economy	IA (Disaster Assistance Improvement Program (DAIP)): TBD IA (National Emergency Management Information System (NEMIS)): TBD PA (Emergency Management Mission Integrated Environment (EMMIE)): TBD	DAIP: High ***IA (NEMIS): Low (In Progress)*** ***PA (EMMIE): Low***

Appendix B
Management Comments to the Draft Report

Mission Modernization Effort	Measures	Examples	Impact
	Efficiency	IA (DAIP): Provides "single point of entry" for services provided by 17 Federal Agencies IA (NEMIS): Capital plan outlines infrastructure improvements. ***Software development placed under management controls in the enterprise software development contract to track project performance.*** ***PA (EMMIE): placed under management controls in the enterprise software development contract to track project performance.***	
	Effectiveness	IA (DAIP): Can be scaled to intake 200,000 registrants in a 24 hour period. Recognized by Federal CIO for its effectiveness as an "intake" point for claimants. Copied for gulf oil disaster. ***IA (NEMIS): Infrastructure improvement planned.*** ***PA (EMMIE): Analysis underway to determine path forward.***	

So how does FEMA manage the *risk* associated with IT modernization efforts in general and the dynamic nature of the mission functional area?[3] It does so with enterprise processes and standards integration with the Department; and management controls, such as Program or Project Management Offices (PMOs), Executive Steering Groups and Committees, and Working Groups that report up the functional leadership chain for decision making.[4] In the tables above, all of the underlined modernization efforts have such a committee or group associated with them. All of the enterprise functional area categories and activities are integrated with and governed by the Department's overall modernization efforts. In some cases, such as e-Mail, computing, and collaboration, FEMA has been the "lead user" for the Department taking the lead to design, develop, test, and implement modernized services that achieve measureable economy, efficiency, and effectiveness *across the Department*.[5] In other enterprise functional area activities, such as network security services, FEMA has integrated with the Department's lead user, Customs and Border Patrol, to achieve measureable economy, efficiency, and effectiveness.

In the business functional area, the TASC steering group governs activities associated with modernization efforts related to the budget, finance, acquisition and property categories. FEMA has a TASC PMO and a steering committee that manages activities within the Agency. Activities associated with the Human Capital category are managed by a Department-level steering group, which is chaired by the Department's Chief Human Capital Officer.[6] The mission functional area, with a few exceptions, follows suit with executive steering groups or PMOs overseeing development and investment decisions. The exceptions, such as Alerts and Warnings, and

[3] One of the major weaknesses in the report's methodology is that it neither addresses putative issues with measures that quantify risk, nor does it offer a basis of comparison for categories such as "economy, efficiency, effectiveness." For example, stating that "the agency should only make investments that move the agency toward a target architecture, which should also be closely aligned with the organization's strategic plan" because of a 1993 law does not offer a quantifiable characterization of risk or a basis for comparison to state whether an organization has made progress in achieving "economy, efficiency, and effectiveness."

[4] Addresses issues identified by the IG in 2006 and 2008.

[5] "Lead User" is a term used to describe organizations or people who are at the forefront of creative problem solving and innovation.

[6] A memorandum issued by the Department's Deputy Secretary further halts all component-independent HC development efforts.

Preparedness, are guided by an Office of Management and Budget approved capital plan (Alerts and Warnings) or have been identified by senior leadership as needing to have formal governance processes instituted (Preparedness).[7]

The aforementioned groups, committees, PMOs, etc., have charters or other types of formal guidance documentation. The FEMA CIO, or an OCIO senior leader, participates actively in each of the groups. Sanctioned IT activities are undertaken within and governed by the framework of the System's Engineering Lifecycle and a common (integrated) set of design, development, test, and implementation standards, and executed within contracts managed or overseen by the OCIO. In this context, (the aforementioned palpable and significant evidence of making progress in achieving "economy, efficiency, and effectiveness" in comparison to previous IG reports; established governance processes; and direct leadership involvement) statements such as "FEMA does not yet have an effective IT strategic plan or completed architecture that can be used to guide and constrain IT development and modernization efforts...." have much less of an impact. The recommendations as stated in the IG report address much less of a risk. In this context the strategy has been set, the "target architecture" has been defined to a workable level of "completeness" or put within manageable parameters, and the investment decision process instituted.

The FEMA CIO recognizes that the aforementioned conditions do not in and of themselves create an ideal IT modernization environment and that challenges remain. For example, FEMA's innovators often expend IT resources without coordinating within their own program offices and without regard for enterprise considerations, such as investment planning and systems integration. Two important examples show that senior leaders recognize this problem. One of the examples is the Department Deputy Secretary's guidance with regard to Human Capital system development efforts. The other, is the FEMA Administrator's, and Associate Administrator for Response and Recovery's guidance regarding the management of the all development activities within FEMA's mission functional area. Both examples recognize the need to "guide" modernization while at the same time meet functional or urgent mission needs. Both examples recognize the universal problem of unsanctioned IT spending and development, and seek to control it.

The challenge for the Agency in this case becomes keeping apace or ahead of and implementing improved technologies to meet dynamic "local" requirements, in the context of enterprise needs, in an environment constrained by monolithic acquisition processes and arcane security standards. The Agency has to cultivate creativity and turn it into IT innovation for the ultimate benefit of a disaster survivor and the enterprise. This challenge requires leadership involvement across the continuum of management levels, rather than a static "complete list of systems" or an ambiguous "complete enterprise architecture." The CIO's oversight responsibilities are one part of a triad, a triad which also includes individual employee personal accountability, and as noted above, involvement across the leadership continuum.

The narrative in the IG report also seems to carry a system's bias, which leads to statements that are not supported by evidence such as, "FEMA Technology Does Not Effectively Support Operations," and other methodological weaknesses.[8] Rather than validating whether a requirement actually exists or a process has been sanctioned by leadership across the enterprise,

[7] See FEMAStat note above.
[8] The focus of the report seems to be on systems rather than validating requirements and improving processes, which points to another weakness in the report's methodology.

Appendix B
Management Comments to the Draft Report

the report cites the example that critical systems such as "ADD" and "LIMS-III" amongst other systems, are not integrated, when in fact the Agency's intended, documented, and leadership-acknowledged "target architecture" does not seek to integrate these two "systems."[9] Recognizing that the requirements and processes for managing deployed personnel were not coherent, and that the functionality ADD provides was probably not sufficient, in Fiscal Year 2010, FEMA's CCHCO and CIO awarded a work order to investigate and address this specific need. The "target architecture" for the property management functionality that LIMS is supposed to support will be implemented in TASC.[10] Continued references to needing to integrate these "systems," indicates that this purported "FEMA IT challenge" was based on incorrect and outdated information.

In summary, the FEMA CIO agrees with the recommendations in general. All well run organizations need to plan, and have foundational documentation and established processes. These items need to be evaluated, refined, and re-communicated continually. The report reminds the CIO that the Agency's IT strategy needs to be updated and re-communicated to FEMA's staff and program offices. Challenges do remain. The CIO disagrees with the characterization of those challenges with regard to IT modernization. The report downplays or ignores significant, quantifiable IT modernization improvements in each of FEMA's IT major functional areas—enterprise, business, mission. And, instead offers no measureable criteria by which to evaluate "economy, efficiency, and effectiveness;" or risk, and refers to anecdotes and anachronistic systems and processes as evidence to support its conclusions.

In this vein, FEMA comments on the report's recommendations are as follows.

Recommendation #1: *Develop a comprehensive IT strategic plan with clearly defined goals and objectives to support program IT initiatives.*

The FEMA CIO suggests changing the recommendation to: *Update the IT strategy that supports the Agency's ongoing and planned mission activities. The IT strategy should show the relationship between the existing IT environment, a desired target state, and the technical standards and guidelines for acquisition and investment decisions.*

Rationale: the revised recommendation captures the essence of recommendations 1, 2, and 3 and focuses on keeping the IT strategy current rather than *completing* it, which in present day terms would be too static, blunt innovation, and not recognize the dynamic nature of mission needs.

Actions the FEMA CIO will take: The FEMA CIO will establish an interactive website that defines *strategic goals* for major functional areas that support *sanctioned* mission goals and needs, and provides links to the modernization management structures and specific activities occurring in those areas. The site will document the existing IT environment, a desired target state, and the technical standards and guidelines for acquisition and investment decisions in those areas. The website will have an interactive process for feedback (WIKI, Blog, etc.). Leaders of individual activities will be responsible for revising the content of their planning, foundational documentation, and established processes, as needed.

Recommendations #2 & 3: *See revised recommendation #1 above.*

[9] ADD refers to the Automated Deployment Database and LIMS-III refers to the Logistics Information Management System III.

Appendix B
Management Comments to the Draft Report

Recommendation #4: *Establish an agency-wide IT budget planning process to include all FEMA program technology initiatives and requirements.*

The FEMA CIO suggests changing the recommendation to: *Enforce the agency-wide budget planning process that guides IT investment decisions.*

Rationale: the revised recommendation recognizes that a process already exists and requires integration of Agency-wide program planning and activities, and involvement across the leadership continuum rather than proscriptive "IT policies."

Actions the FEMA CIO will take: The FEMA CIO will continue to meet with senior leaders in enterprise, business, and mission areas to ensure IT investments support Agency mission goals. Meetings will be held on a quarterly basis and the results of the meetings will be posted to the interactive IT strategy website.

Recommendation #5: *See revised recommendation #4 above.*

Recommendation #6: *See revised recommendation #1 above.*

Appendix C
Major Contributors to this Report

Information Management Division

Richard Harsche, Division Director
Kristen Evans, Audit Manager
Swati Nijhawan, Auditor-in-Charge
Erin Dunham, Auditor
BriElle Bryson, Intern
Thomas Rohrback, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
FEMA, Administrator
FEMA, Deputy Administrator
FEMA, Chief Information Officer
Acting Deputy Director of External Affairs
Deputy Director of the Office of Policy & Program Analysis
FEMA Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or 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.