DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery

Office of Information Technology

OIG-05-36

September 2005

Office of Inspector General

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

Homeland Security

Preface

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

This report assesses the strengths and weaknesses of the information technology that the Emergency Preparedness and Response Directorate uses to support incident response and recovery operations. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

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

Richard L. Skinner
Inspector General

Contents

Appendices

Abbreviations

ADD	Automated Deployment Database
CIO	Chief Information Officer
DHS	Department of Homeland Security
EP&R	Emergency Preparedness and Response Directorate
FEMA	Federal Emergency Management Agency
GAO	Government Accountability Office
IFMIS	Integrated Financial Management Information System
IT	Information Technology
LIMS III	Logistics Information Management System III
NEMIS	National Emergency Management Information System
OIG	Office of Inspector General

Contents

Figures

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

Providing disaster recovery assistance and responding to the emergency needs of victims of four consecutive hurricanes in 2004 was a major challenge for the U.S.[1] When devastation from such incidents is so great that state resources cannot handle the response and recovery efforts, states turn to the federal government for assistance. The Federal Emergency Management Agency (FEMA), now part of the Emergency Preparedness and Response (EP&R) Directorate of the Department of Homeland Security (DHS), is responsible for coordinating disaster relief efforts across federal, state, and volunteer organizations, such as the American Red Cross. FEMA relies heavily on a range of information technology (IT) systems and tools to carry out its response and recovery operations. Strategic management of these assets is important to ensure that the technology can perform effectively during times of disaster and tremendous stress.

As part of our ongoing responsibility to assess the efficiency, effectiveness, and economy of departmental programs and operations, we conducted an audit of the information and technology that EP&R uses to support incident management. The objectives of the audit were to (1) review the directorate's approach for responding to and recovering from terrorist attacks, major disasters, and other domestic emergencies, (2) determine the effectiveness of guidance and processes to support IT users during incident management, and (3) evaluate existing and proposed systems and other technologies used to accomplish EP&R's response and recovery mission. The scope and methodology of this review are discussed in Appendix A.

Strategic IT management is essential to the successful accomplishment of EP&R's response and recovery mission. EP&R's IT approach has met the disaster management challenges to date, including the four major hurricanes of 2004. However, a number of information and technology management issues limit the directorate's effectiveness.

[1] The 2004 hurricanes that made landfall in Florida and the Gulf Coast included Charley on August 13th, Frances on September 5th, Ivan on September 16th, and Jeanne on September 26th.

For example, the EP&R Chief Information Officer (CIO) is making progress with respect to IT planning, including the development of the agency's first IT strategic plan. However, while the IT plan aligns with FEMA's outdated strategic plan, it does not reflect FEMA's integration into DHS and therefore may not support DHS' strategic goals. Additionally, to better align EP&R's IT with the agency's strategic direction, integration with evolving DHS-wide initiatives, such as *eMerge*^{2} and *MAX*^{HR}, will prove challenging.

Further, EP&R CIO support to IT users could be improved. EP&R CIO staff, including the national IT helpdesk, provided significant service during the 2004 hurricanes. However, additional guidance and training for systems users is necessary to ensure that they have the knowledge and information needed to perform their jobs. The EP&R CIO's office maintains up-to-date—and often online—systems procedure manuals and guidance, but FEMA field personnel are often unaware of these materials. In addition, the IT manuals online describe the procedures necessary to complete actions in the systems, but they do not contain the business context for when or how the procedures should be used. Although EP&R's custom, complex systems require significant amounts of front-end instruction, users said that they received insufficient training.

Currently, EP&R systems are not integrated and do not effectively support information exchange during response and recovery operations. Also, EP&R has not fully updated its enterprise architecture to govern the IT environment. As a result, during significant disaster response and recovery operations, such as the 2004 hurricanes, IT systems cannot effectively handle increased workloads, are not adaptable to change, and lack needed real-time reporting capabilities. Such problems usually are due to FEMA's focus on short-term IT fixes rather than long-term solutions. Inadequate requirements definition, alternatives analysis, and testing prior to systems deployment are characteristics of this reactive IT management approach.

Although EP&R is working to introduce and web-enable systems to resolve disparity between its current IT environment and DHS expectations, additional measures are needed. EP&R would benefit from strategically managing IT by aligning its IT planning with DHS' direction as well as ensuring systems users receive more timely training and communication. Further, once broad-based requirements are fully defined and documented, and alternatives are analyzed, EP&R will be in a better position to complete an enterprise architecture, and test and deploy the most appropriate technology needed to support its response and recovery mission.

Background

Following the terrorist attacks of September 11, 2001, DHS was established to prevent and deter terrorism, and to protect against and respond to threats and hazards to the nation. The *Homeland Security Act of 2002*[2] assigns responsibility to the EP&R directorate to lead federal disaster response and recovery activities. FEMA, transferred in its entirety into the EP&R directorate, is directly responsible for executing this aspect of DHS' mission. The organization chart below illustrates EP&R and FEMA within the context of the DHS organization. (See Figure 1).

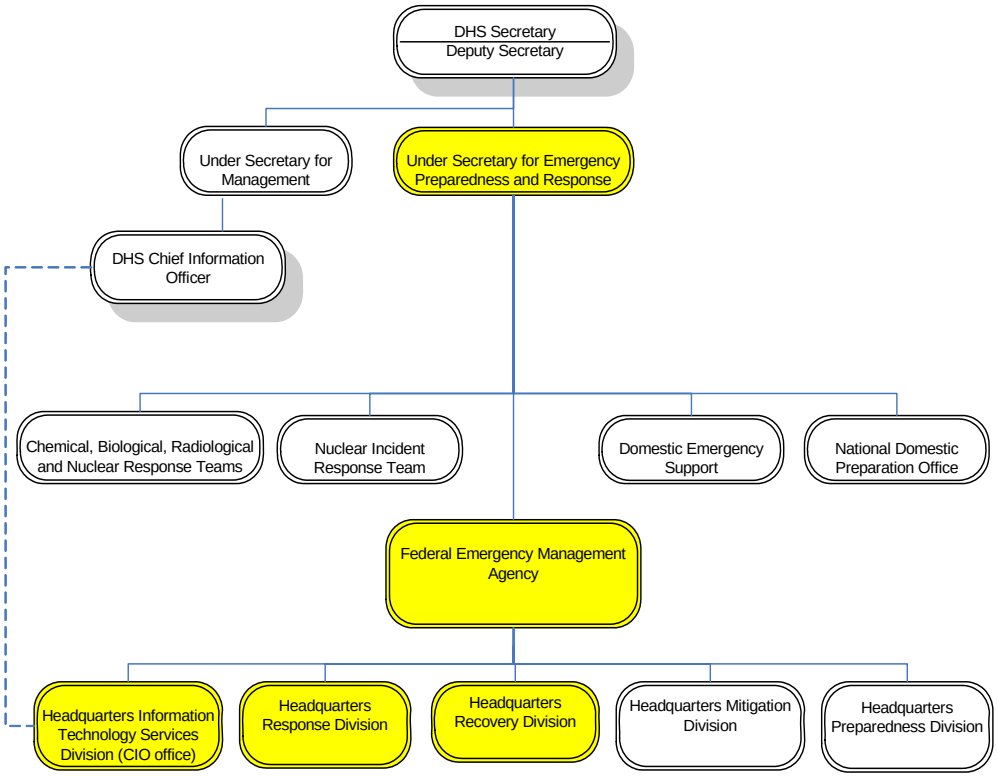

Figure 1: EP&R/FEMA Organization

When devastation exceeds the capability and resources of local and state governments to respond they turn to the federal government for assistance. The *Stafford Act*[3] gives FEMA the authority to lead the disaster response and

[2]Public Law 107-296, November 25, 2002.
[3] *Robert T. Stafford Disaster Relief and Emergency Assistance Act,* as amended by Public Law 106-390, October 30, 2000.

recovery operations of 28 major federal agencies and departments, the American Red Cross, and other volunteer organizations. FEMA supplies immediate needs, such as ice, water, food, and temporary housing. FEMA also provides financial assistance to individuals who have sustained damage to their personal property, and to state and local governments for damage to public property.

FEMA has ten regional offices across the country to assist the states in disaster management. The map below depicts this regional office structure. (See Figure 2).

Figure 2: FEMA Regional Offices

Emergency and IT Support Capabilities

EP&R provides an array of emergency operations, facilities, and systems to help manage disasters. FEMA has four National Processing Service Centers which handle telephone registration and process victims' claims for disaster assistance, as well as five geographically-dispersed Mobile Emergency Response Support operations which provide initial support for on-site disaster management. This mobile support includes providing voice, data, and video capabilities for emergency managers, as well as services such as water purification and power generation. Immediately following this initial response, FEMA establishes disaster field offices and disaster recovery

centers to assist victims on a long-term basis. Emergency operations centers at FEMA headquarters and at the Mount Weather facility near Bluemont, Virginia, coordinate response and recovery operations nationwide.

In FY 2005, the EP&R directorate's CIO had a budget of approximately $80 million and a total of about 400 full-time and temporary employees. The CIO's office is responsible for designing, developing, testing, implementing, and maintaining the operation of FEMA's systems, including the following four key applications:

- National Emergency Management Information System (NEMIS) is the backbone IT system for response and recovery operations. FEMA uses NEMIS to electronically enter, record, and manage information regarding registered applicants for disaster assistance, obligations and payments, mission assignments, and grants.

- Integrated Financial Management Information System (IFMIS) forwards financial information to the Department of Treasury for payment of disaster assistance claims.

- Logistics Information Management System III (LIMS III) maintains the inventory of equipment and supplies.

- Automated Deployment Database (ADD) is used to identify and deploy personnel to disaster sites.

With the exception of NEMIS, these systems were not developed by and do not solely belong to IT. However, IT partners with EP&R program areas in providing support for these systems.

The CIO's office manages and maintains the IT infrastructure, i.e., networks, databases, desktops, and telephone systems, to support operations of permanent facilities at FEMA headquarters and regional locations. The CIO also is responsible for providing the IT infrastructure to support hundreds of emergency personnel at temporary disaster field offices and recovery centers, often in remote locations. This involves running cable, establishing networks, supplying wireless connectivity, and installing equipment for information processing and data and voice communications. In addition, a national IT helpdesk assists users in various ways such as providing and maintaining system accounts, ensuring remote access, troubleshooting systems problems, and making referrals to engineers for systems fixes.

Prior assessments have identified concerns with several aspects of FEMA's IT management. Specifically, in an August 2001 report,[4] the GAO identified issues with NEMIS internal controls, reliability, usability, and training. A July 2004 GAO report[5] discussed FEMA's property management controls and highlighted concerns with asset accountability and the accuracy of data recorded in the LIMS III system. In that report, GAO recommended that FEMA's property system be linked to its acquisition and financial systems so that certain key information could be available for effective property management. In December 2003, we issued a report[6] on the NEMIS system access controls, and identified related issues concerning separation of duties, audit trails, and training which needed to be monitored. Further, a July 2004 DHS OIG report[7] discussed the need for component CIOs, such as the EP&R CIO, to report to the department's CIO on IT issues to help ensure that strategies are aligned and systems are consolidated for more effective use of IT assets across the department.

Results of Audit

Challenges Remain in Aligning EP&R's IT Approach with DHS Mission

Information resource management plans support an agency's strategic plan for fulfilling its mission. The 2004 DHS strategic plan contains specific response and recovery goals and metrics. FEMA's strategic plan, however, is not aligned with them. FEMA developed its strategic plan prior to becoming part of the new department and has not updated it since then. EP&R's IT plan aligns with FEMA's outdated plan, but does not line up fully with goals and measures defined in the more recent DHS plan. As a result, EP&R's IT systems approach may not support progress toward meeting DHS goals. Updating its strategic and IT plans to reflect evolving DHS-wide direction and initiatives poses a major challenge for EP&R.

[4] *Disaster Assistance: Improvement Needed in Disaster Declaration Criteria and Eligibility Assurance Procedures*, GAO-01-837, August 2001.
[5] *Federal Emergency Management Agency: Lack of Controls and Key Information for Property Leave Assets Vulnerable to Loss or Misappropriation*, GAO-04-819R, July 2004.
[6] *Audit of the National Emergency Management Information System Access Control System*, DHS-OIG-04-02, December 2003.
[7] *Improvements Needed to DHS' Information Technology Management Structure*, DHS-OIG-04-30, July 2004.

Strategic and IT Plans Not Fully Aligned

FEMA's strategic and IT plans do not align completely with DHS' strategic plan, providing little assurance that the agency can monitor and achieve the emergency management goals established by the department. Pursuant to requirements of the *Government Performance and Results Act of 1993*,[8] DHS developed its strategic and performance plans which, taken together, establish its mission and outline goals and metrics for its disaster response and recovery efforts. According to the EP&R CIO, FEMA participated in working groups to help develop these DHS goals and objectives and owns all the metrics that support the response and recovery section of the DHS strategic plan. Goals in the plans include leading, managing, and coordinating the national response and recovery effort, and rebuilding communities after acts of terrorism, natural disasters, or other emergencies. Corresponding metrics include reducing response time for emergency personnel deployment and logistics as well as reducing recovery assistance delivery costs and processing time. The following diagram illustrates the alignment between these goals and metrics to help ensure effective and efficient mission accomplishment. (See Figure 3).

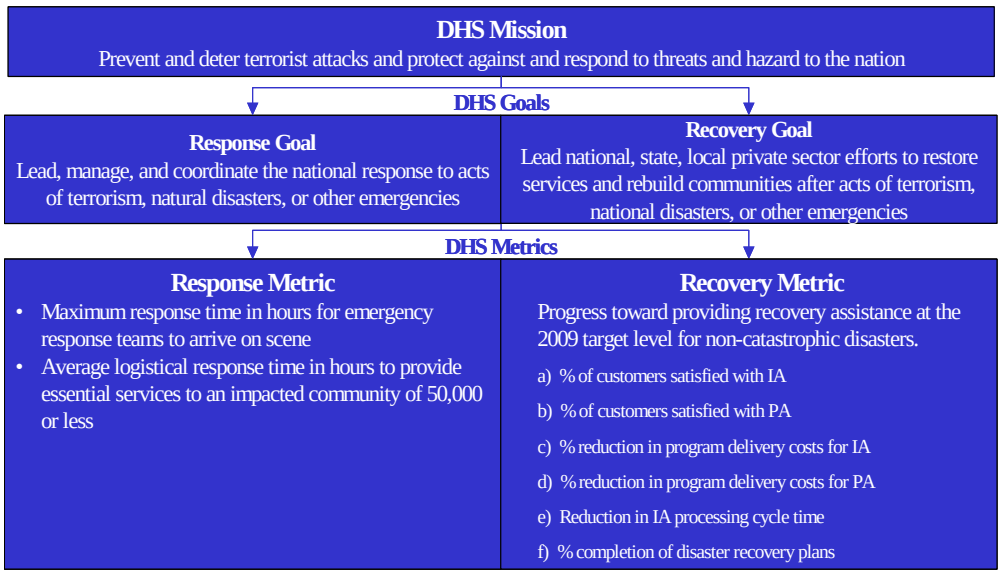

Figure 3: DHS Mission and Response and Recovery Goals and Metrics

Although Office of Management and Budget Circular A-11 directs that component agencies create their own strategic plans linked to overarching

[8]Public Law 103-62.

departmentwide plans, FEMA has not updated its strategic plan to reflect its integration into the DHS organization.[9] FEMA developed its strategic plan prior to implementation of the *Homeland Security Act* and the creation of DHS. DHS has established specific metrics for response and recovery response time, customer satisfaction, program delivery cost, and disaster assistance cycle time. However, as demonstrated in Figure 4, FEMA's strategic plan fails to identify such metrics, and therefore is not in line with DHS direction.

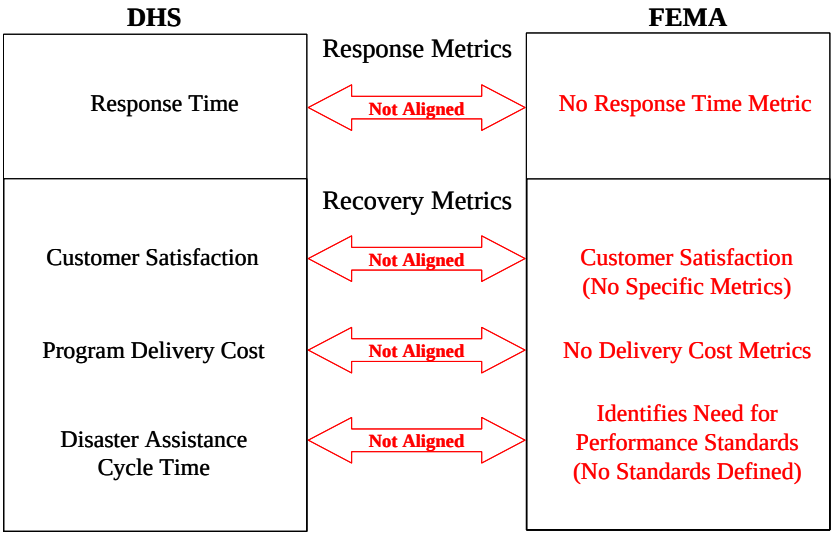

Figure 4: DHS and FEMA Response and Recovery Metrics Not Aligned

A planning official said that FEMA uses both the DHS strategic plan and FEMA's outdated plan. Use of both plans may lead to ambiguous guidance and direction. For example, the two plans identify different metrics to measure improvement in the federal government's ability to respond quickly when states are overwhelmed by a disaster. The DHS plan sets the goal of 12-hour response time for emergency response teams and 24-hour logistics response time by 2009. In contrast, FEMA's plan establishes a goal to respond concurrently to four catastrophic and twelve non-catastrophic disasters by 2008. Although it began updating its strategic plan in mid 2004 to reflect the organizational changes and new performance expectations,

[9] Circular A-11, Part 6, *Preparing and Submitting a Strategic Plan*, Executive Office of the President, Office of Management and Budget, June 2005.

FEMA put the updates on hold due to the need to shift resources to the 2004 hurricane response and recovery activities.

Further, the misalignment of DHS and FEMA strategic plans complicates efforts to link IT initiatives to overarching mission direction. According to the *Paperwork Reduction Act*[10] and the supporting Office of Management and Budget Circular A-130[11], each federal agency is required to develop an Information Resource Management Plan to demonstrate how IT management activities help accomplish an agency's mission. The EP&R CIO accomplished an important step by implementing FEMA's first IT strategic plan for FY 2005. However, the CIO's IT plan maps to FEMA's outdated strategic plan rather than to the more recent DHS strategic plan. For example, the IT plan identifies six strategic management initiatives, which it aligns to the goals identified in the FEMA strategic plan; however, the initiatives do not align completely to goals and metrics identified in DHS level planning. As a result, the initiatives defined by the CIO organization may not support the achievement of the response and recovery goals and metrics established by DHS.

Performance Data Not Available from Systems

Federal regulations, including the *Paperwork Reduction Act*, require agencies to use information resources to improve the efficiency and effectiveness of their operations to fulfill their missions. However, EP&R's IT systems do not provide the data needed to support the response and recovery metrics established by DHS effectively. Some of the metrics are IT-dependent, reliant upon automated systems to capture quantifiable information with which to measure performance in specific response and recovery activities. Where IT systems do not provide the data for measuring performance, it is not possible successfully to measure progress toward the achievement of specific goals, and ultimately the agency's mission.

Response Metrics

With regard to disaster response, DHS' strategic plan identifies specific performance indicators, such as the time it takes to deploy personnel and assets to aid in a disaster. In 2004 DHS allotted 72 hours for providing both

[10] Public Law 104–13, May 22, 1995.
[11] Circular A-130, *Memorandum for Heads of Executive Departments and Establishments, Management of Federal Information Resources*, Executive Office of the President, Office of Management and Budget, February 8, 1996.

emergency teams and essential services[12] to disaster areas; DHS expects to significantly reduce this response time by 2009. The following diagram illustrates DHS' performance objectives for FEMA response time. (See Figure 5).

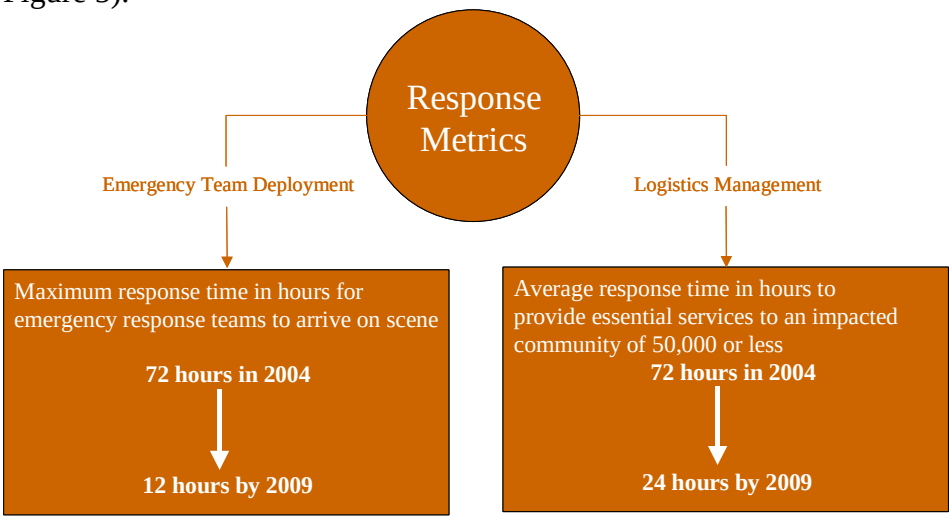

Figure 5: DHS Target Response Metrics

However, measuring response time and progress toward achieving DHS targets is problematic. FEMA's systems for personnel deployment and logistics do not easily track performance information. ADD, for example, does not capture data on how long it takes for emergency personnel to arrive at a disaster site. In other words, the system does not have a "stopwatch" to measure the elapsed time between contacting personnel of their need to deploy and their ultimate arrival at a disaster scene. Currently, program officials must review information manually tracked either on paper or on spreadsheets to determine response time, a very inefficient process. EP&R plans to develop a new deployment management system to address this issue.

Similarly, LIMS III provides no tracking of essential commodities, such as ice and water, needed by disaster victims. As a result, FEMA cannot readily determine its effectiveness in achieving DHS' specific disaster response goals and whether or not there is a need to improve. FEMA is currently working to establish a baseline for average response time in providing essential services, beginning in 2006. FEMA officials said that they are pilot-testing a Total Asset Visibility system to track shipment and distribution of essential commodities such as ice, water, and food.

[12] Essential services are generally defined as life-saving commodities and emergency supplies including water, food, ice, medical supplies, mobile homes, travel trailers, or other housing options.

Recovery Metrics

With regard to disaster recovery, DHS' strategic plan identifies specific measures for delivering services to disaster victims. Although no baselines are available on the average cost or cycle time for providing assistance, DHS expects to reduce these averages by several percentage points by 2009. The diagram below identifies the performance goals for 2009. (See Figure 6).

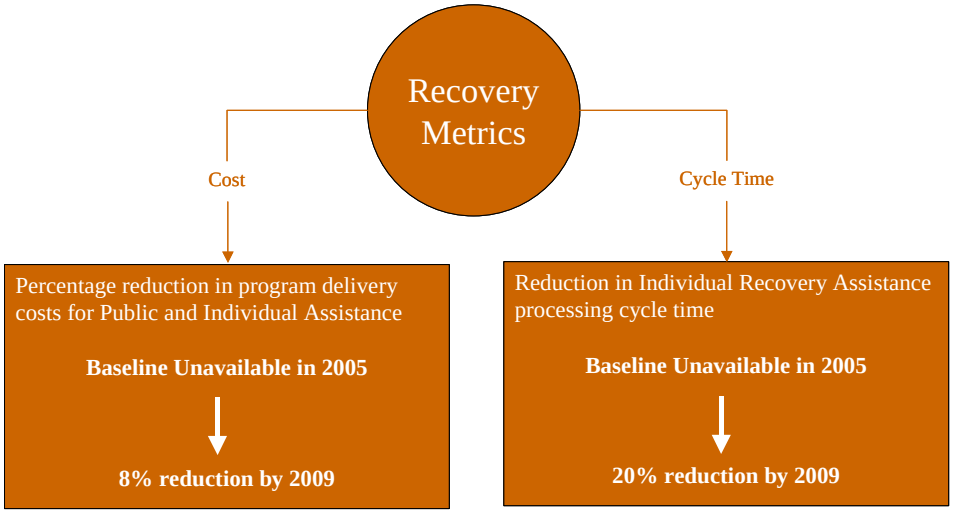

Figure 6: DHS Target Recovery Measures

However, such goals are futile without effective means to accomplish them. Currently, EP&R IT systems provide limited data to measure recovery assistance performance. For example, EP&R's Recovery Division is using IFMIS to capture unit cost data on recovery assistance. However, according to several FEMA officials, this data is not available at a single point in IFMIS and must be manually calculated. Compiling this data requires significant time, effort, and resources because information for establishing unit costs for rent, IT, security, and other elements is pulled from different systems and files.

Similarly, FEMA is working to establish a baseline for the average cycle time from a victim's initial registration until disaster assistance payments are issued. Program officials said that, although NEMIS collects information on cycle time, this information is not readily or routinely available. These officials said that they must request EP&R's IT division to access the system and compile weekly ad hoc reports to provide the information. Program officials said that additional information on subcomponents of the cycle time

would be useful, such as how long it takes a victim to register or get an inspection after registration.

Officials in EP&R's Recovery Division said that they are working to establish baselines this year against which to measure progress in reducing cost and time for delivering individual and public assistance. However, until FEMA's systems can capture the underlying performance data, the agency will be unable to do so.

Challenges in Aligning IT with Evolving DHS Direction

In addition to addressing the need to align its strategic and IT planning with DHS direction, EP&R faces the challenge of integrating its emergency management approach with several emerging departmentwide initiatives. Specifically, DHS implementation of the National Response Plan and the National Incident Management System created new requirements that will affect IT systems and processes. Additionally, the DHS Chief Financial Officer's efforts to provide integrated resource management must be taken into consideration as EP&R moves forward in its approach to managing IT.

Impact of the National Response Plan and National Incident Management System on EP&R IT

The National Response Plan provides the framework for federal coordination with state, local, and tribal governments, as well as the private sector during disasters. DHS implemented the National Response Plan in December 2004, according to the *Homeland Security Act of 2002* and *Homeland Security Presidential Directive 5.*[13] The National Response Plan consolidates existing federal government emergency response plans into a single, coordinated plan to manage disaster response and recovery. This consolidated plan replaces the Federal Response Plan, which FEMA previously used as the basis for organizing its response and recovery operations. The new plan introduces changes to the organizational structure for disaster management operations, and will require software code updates to information systems.

For example, the NEMIS Access Control System assigns access rights to users based on positions within the organization structure, which are defined in the former Federal Response Plan. Moving to the National Response Plan has changed this organizational structure and, consequently, affected NEMIS Access Controls, requiring that new roles and rights be added to the system

[13] "Management of Domestic Incidents," Homeland Security Presidential Directive 5, February 28, 2003.

before NEMIS can be used to support the plan. One FEMA official was concerned that there are no funds available for correlating the organizational changes with IT processes. This official was unaware of any IT involvement in the National Response Plan development process. Consequently, FEMA's IT managers now must identify ways to adapt existing systems to meet new response plan requirements.

In conjunction with the National Response Plan, DHS developed the National Incident Management System in 2004 to provide guidance, such as common terminology and organizational processes, to enable first responders at all government levels to work together effectively during disasters. First responders include federal, state, local, and tribal governments and private sector and nongovernmental organizations. The National Incident Management System policy requires inter-operability of response structure, equipment, communications, qualifications, and certifications. According to National Incident Management System guidelines, maintaining an accurate picture of resource utilization is a critical component of incident management. The system requires standardized resource management across various first responder entities, as well as asset tracking over the lifecycle of an incident.

LIMS III, FEMA's current logistics system, does not provide the type of up-to-date resource management that the National Incident Management System requires. Resource tracking and management was the source of numerous problems during the Florida hurricanes, as will be more fully discussed in later sections of this report. However, not only is LIMS III not integrated with other systems within FEMA, it does not provide the capability to view and share resource information across federal, state, and local first responders. Personnel at nearly all sites that we visited commented on the need for an improved resource tracking system to support NIMS. A FEMA official said that system capacity requirements do not reflect the catastrophic magnitude of today's threats, and that system upgrades and integration have not kept pace with recent organizational, business process changes, or operational concepts.

Departmentwide Initiatives Affect EP&R IT—

DHS is developing two new departmentwide systems that have implications for EP&R IT management. Specifically, *Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency*, known as *eMerge*^{2}, is an ongoing project to consolidate and integrate DHS' budget, accounting and reporting, cost management, asset management, and acquisitions and grants functions. In conjunction with *eMerge*^{2}, DHS is also developing a departmentwide integrated human resource management system, the *MAX*^{HR}

project. Taken together, the two projects will affect several of FEMA's major response and recovery IT systems. For example, *eMerge*^{2} will affect aspects of FEMA's financial system, as well as parts of its non-mission specific logistics system. Likewise, *eMerge*^{2} is likely to have an impact on NEMIS' grants functionality. Further, *MAX*^{HR} may have a bearing on employee management and deployment processes currently managed in ADD.

Once fully implemented, *eMerge*^{2} will likely affect FEMA's current financial system, grants management system, and aspects of its non-mission specific logistics system. Although FEMA officials have actively participated in the DHS Logistics Steering Committee to define *eMerge*^{2} development, some officials have expressed concern that the *eMerge*^{2} effort does not address some of their requirements. For example, these officials said that *eMerge*^{2} does not consider the complexity of FEMA's disaster grants programs as compared with standard grants processing. The limited time and resources to successfully plan and transition to *eMerge*^{2} also troubled them. Conversely, *eMerge*^{2} officials expressed concern that FEMA was not open to new ways of thinking. As FEMA moves forward with improving existing systems and pursuing new systems development, the EP&R CIO must continue to ensure that the effects of DHS-wide initiatives, such as *eMerge*^{2} and *MAX*^{HR}, are considered and effectively support disaster response and recovery goals.

Recommendation

1. We recommend that, in keeping with legislative requirements, the Under Secretary for EP&R update the FEMA strategic plan to support achievement of DHS goals and ensure that all FEMA systems provide the performance data necessary to measure progress toward achieving response and recovery goals. Subsequently, direct the EP&R CIO to update the IT strategic plan in line with the updated FEMA strategic plan.

IT User Support Could Be Improved

The EP&R CIO's office provided significant customer support to IT users assisting disaster response and recovery efforts related to the 2004 Florida hurricanes. However, overall systems guidance and training could be improved. Specifically, EP&R has reasonably up-to-date online systems manuals, but these manuals are not adequate to support business processes. Often unaware of the online manuals, field personnel used out-of-date hard copy guidance to meet their needs. Although a number of users said that

EP&R training is good, funding restrictions limited the number of personnel who received it, resulting in a lack of awareness of how the systems function and a low comfort level in using those systems. Additional systems guidance and training for IT users would provide users with the information they need to perform their jobs better.

IT Support During the Florida Storms

The concurrent hurricanes which struck Florida and the Gulf Coast in 2004 pushed FEMA's IT capabilities to the limit, demonstrating the agency's commitment to carrying out its mission regardless of the adversities encountered and the enormous effort required. Hurricanes Charley, Frances, Ivan, and Jeanne—all category three or stronger storms—along with Tropical Storm Bonnie, hit the region in close proximity and within a few weeks of each other.[14] Figure 7 illustrates the date and location of these storms, which collectively created near-catastrophic conditions and caused an estimated $42 billion worth of damage. FEMA defines a catastrophe as an incident which results in extraordinary levels of damage and almost immediately exceeds state and local resources and significantly interrupts governmental operations and emergency services.

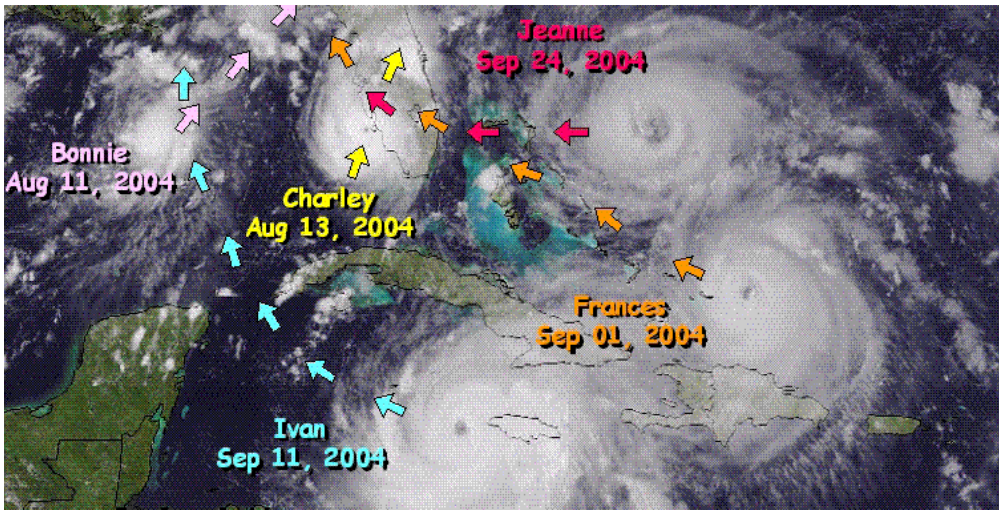

Figure 7: Four Category 3+ Hurricanes in 2004

[14] The Saffir-Simpson Hurricane Scale defines hurricane intensity using a rating scale of 1-5, where 1 is the least intense and 5 is the most intense. Hurricanes Charley and Frances were category 4 hurricanes, with wind speeds of 131-155 miles per hour. Ivan and Jeanne were category 3 hurricanes at landfall, with wind speeds of 110-130 miles per hour.

Under the circumstances, EP&R CIO IT support staff provided significant service during the Florida hurricanes of 2004. FEMA IT was tasked to establish quickly a 200,000 square foot disaster field office—the largest in its history—within just seven days. Approximately 2,000 employees staffed this disaster field office. Previously, a field office of just 400-500 employees was considered large; accordingly, NEMIS was designed to support a maximum of three disaster field offices of 150 employees each. (See Figure 8). Significant IT resources were required to set up phone and data lines and computer stations, and to manage system access rights for system users. Providing system and network support for such a large operation proved challenging.

For example, during the hurricanes, NEMIS handled more than one million requests for disaster assistance in just six weeks. Due in large part to NEMIS automation, individual assistance was generally provided within 7 to 10 days as compared to several weeks via the predecessor system. NEMIS and its support staff were stretched to the limit and demonstrated remarkable dedication to sustaining operations where systems access and capabilities far exceeded systems design. At one point, NEMIS supported 18 call centers, well beyond its design requirement of three call centers and 20,000 calls per day. Overall disaster victim satisfaction with call center service was about 85 percent, despite this large volume of calls.

Figure 8: Disaster Field Office in Orlando, Florida

The national IT helpdesk also provided effective support for FEMA's disaster management operations in Florida. During FY 2004, largely due to the concurrent hurricanes, the helpdesk handled a 50 percent increase in call

volume, with 33,000 calls received over the course of the year. FEMA personnel in both the regional and the disaster field offices reported that the IT help desk at Mount Weather provided excellent support. The helpdesk supports all areas of IT, including dial-up access, account access for new users, troubleshooting, and remote access. The views of personnel with whom we spoke were substantiated by a client satisfaction survey conducted during 2004 by the Customer Care Institute, an external firm specializing in customer satisfaction surveys. The response rate was 37 percent, or 302 of the 816 clients surveyed. The survey results helped identify current client satisfaction levels, as well as establish a benchmark for future surveys. According to the survey, approximately 97 percent of the respondents were satisfied with the service that they received from the helpdesk, and 46 percent were extremely satisfied.

Additional IT Guidance and Training Needed

According to *Office of Management and Budget Circular A-130*, users of federal information resources must have the skills, knowledge, and training to manage information resources, enabling the federal government to serve the public through automated means. According to the *Clinger-Cohen Act of 1996*,[15] agencies are responsible for ensuring that IT users receive the training that they need to do their jobs. Although EP&R's IT technical support personnel responded effectively to system user needs, especially prior to and during the Florida disasters, additional guidance and training for system users is necessary to ensure that users have the knowledge and information necessary to perform their jobs efficiently and effectively.

Specifically, although the EP&R CIO's office maintains up-to-date systems procedure manuals and guidance, such as online job aids, a number of FEMA field personnel whom we interviewed were not aware of their existence. Unaware of online resources, users relied on out-of-date manuals or created their own individual reference documents: two of the three regions that we visited were using out-of-date, hard copy systems manuals that were still in draft format.

In addition, the online IT manuals only described the procedures necessary to complete actions in the systems; they did not contain the business context for when and why the procedures would be used. This information, provided in separate manuals created by the program areas, forced system users to refer to

[15] Sections D and E of Public Law 104-106.

two different sources to obtain an understanding of how to perform their jobs. For example, if a manager wanted to create a mission assignment in NEMIS, that manager would need to refer to a program-created guide, *Mission Assignment for Managers Student Manual,* to understand "when" to create a mission assignment, and to the online system steps to understand "how" to create the mission assignment in NEMIS.

Further, system users were not provided with adequate training. EP&R systems often are custom designed and complex, requiring significant upfront training to understand how to use them to support emergency management activities. Regional system users, however, said that new employees often did not receive training before they were deployed and experienced users did not receive training when system changes occurred.

An independent contractor, charged with documenting and evaluating response and recovery processes during the hurricanes**,** reported that new employees were deployed to the disaster site without first receiving system training. The new employees had to be trained by other FEMA employees during ongoing response and recovery operations. While training new employees onsite at times may be the only option, the problem was that they sometimes relied upon experienced system users that had not received training on system changes and updates. The users, consequently, were not aware of all system functions and had a low comfort level in using the systems.

FEMA regional personnel said that a lack of funding was a reason for the limited NEMIS training. They said that they primarily learned to use the system through on-the-job training rather than through formal instruction. This lack of training had an even greater impact on temporary disaster assistance employees. Sufficient training would have made their work more reliable and much easier.

Recommendation

2. We recommend that, in keeping with legislative requirements, the Under Secretary for EP&R direct the EP&R CIO to ensure that personnel, through the EP&R training division, receive adequate systems training, guidance, and communication needed to support disaster response and recovery activities effectively.

Systems to Support Response and Recovery Operations Need Improvement

Federal regulations require agency CIOs to promote the effective and efficient design and operation of major information resources management processes. They must develop, maintain, and facilitate the implementation of integrated IT architectures to meet agency missions. The EP&R systems environment, however, is not integrated and does not support effective information exchange. Consequently, during disasters, the systems are not able to handle increased workloads effectively, are not adaptable to change, and lack needed capabilities. The reactive nature of EP&R's disaster response encourages short-term systems fixes rather than long-term IT solutions. Taking the time to define and document systems requirements fully and evaluate viable alternatives to its complex, custom designed systems, will enable EP&R to support its response and recovery operations and meet its mission needs better.

Unintegrated IT Environment

EP&R is working to complete an enterprise architecture to govern its IT environment. Currently, however, its systems are unintegrated and do not effectively share information. IT officials agree that it is essential to integrate systems to support mission requirements better, but that decision must be made in collaboration with the systems owners and program officials. Linking the systems to state emergency management systems that rely upon FEMA information to carry out state disaster management responsibilities would also be beneficial.

FEMA Enterprise Architecture Development is Ongoing

The *Clinger-Cohen Act of 1996*[16] requires the CIO to develop, maintain, and facilitate the implementation of a sound, enterprisewide IT architecture. An enterprise architecture provides a blueprint of the hardware, software, and related policies needed to achieve defined business objectives. Such an architecture serves as the agency's road map to future systems development, network updates or changes, and implementation of key federal requirements. In 2001, FEMA developed an enterprise architecture document to serve as a guide to creating and implementing e-government initiatives. This road map has served FEMA well, documenting both major successes and key initiatives. For example, a few such initiatives were identified in the 2001 enterprise architecture and are still operational today. These initiatives include:

[16] Public Law 104-106

- The FEMA website (www.fema.gov), which was developed to share information on the internet with the public.
- The automation of grants management, which has been added to the NEMIS system.
- The development of a capital planning and investment control process, which provides guidance for investment in IT.
- The use of wireless technologies to improve mobile computing and communications support for FEMA operations.

FEMA published its architecture in 2001, but has not fully updated it to reflect its integration into DHS. FEMA is working to transition this paper-based document to an electronic format so that it can be easily shared among DHS officials via the intranet. The EP&R CIO established an Enterprise Architecture Office in 2003 and hired a Chief Enterprise Architect in 2004 to help further the progress of FEMA's enterprise architecture program. The Enterprise Architecture Office has completed the "as is" portion of the enterprise architecture and has begun to use an electronic version to guide day-to-day operations.[17] FEMA is currently working to develop the "to be" portion of the enterprise architecture in line with the DHS enterprise architecture.[18] Without a defined "to be" environment, FEMA is unable to provide a comprehensive road map for its proposed IT initiatives. These initiatives include NEMIS web enablement, which involves consolidation of some of the geographically-dispersed servers, as well as a number of IFMIS improvements as defined in the system's 2006 business case.

Additionally, without a complete, communicated, "to be" road map, FEMA may not be able to address how its initiatives support or integrate with DHS-wide initiatives. As FEMA works to update its enterprise architecture, it must also consider departmentwide initiatives, which may impact on its key response and recovery processes and systems.

Centralization of NEMIS Servers

The *Office of Management and Budget Circular A-130* requires agencies to develop information systems to facilitate interoperability across networks of

[17] An "as is" enterprise architecture details an organization's mission, organizational structure, business processes, information exchanges, software applications, and underlying technical infrastructure.

[18] A "to be" enterprise architecture describes an organization's desired architecture for meeting strategic goals and future needs.

heterogeneous hardware, software, and telecommunications platforms. However, FEMA's current server architecture does not effectively support operations.

When NEMIS was developed, FEMA created a state-of-the-art, distributed client-server architecture, providing each region with its own set of servers to support regional operations. However, as system usage has increased FEMA has recognized the need to move toward a more centralized database structure, and is in the process of consolidating its data storage systems. Such centralization would help ensure data consistency, use less bandwidth, and facilitate backup recovery because the information would be readily available in one place. Presently, information on regional servers must be replicated across multiple servers at FEMA headquarters—a process that delays data exchange and consumes bandwidth. FEMA's limited bandwidth could better be used for advanced technologies such as video teleconferencing, which directly support the agency's emergency management mission. Although, EP&R CIO is in the process of centralizing and consolidating servers, as of April 2005, this process had not been completed. As a result, users continue to experience slow and sometimes unavailable systems. Additionally, if systems were to crash and EP&R were required to recover information or data from backups, it would take as long as a month to complete.

Systems Integration and Information Sharing Need Improvement

According to the DHS strategic plan, DHS will "lead, manage, and coordinate the national response to acts of terrorism, natural disasters, or other emergencies." To accomplish this, DHS has to bring the right people and resources to bear where and when they are needed most, as well as provide integrated logistical support to ensure rapid response and coordination among federal, state, and local operations centers. However, FEMA's systems do not support effective or efficient coordination of deployment operations because there is no sharing of information.

Specifically, NEMIS—the system for managing mission assignments—does not share information with the ADD or LIMS III deployment systems. When a disaster occurs, FEMA and state officials must quickly identify the people and other resources needed to respond to the incident. Information on the disaster is established in NEMIS, including requests for assistance, requisitions and commitments for services and supplies, and the initial allocation of funds. However, FEMA is unable to match automatically the mission assignments in NEMIS to either the personnel deployed through ADD or to the equipment and supplies dispatched through LIMS III. To

compensate, regional staff create and maintain ad hoc databases, spreadsheets, and paper records to manage deployments. During the Florida hurricanes, for example, the regional office in Atlanta, Georgia received from 300 to 400 requests for personnel and supplies within a three-to-four-day period. To respond to these requests, the region improvised by creating a mission assignment spreadsheet that showed the dates and status of the requests, as well as the dates and times that the resources would be received. The spreadsheet enabled the region to coordinate the response and identify those requests that had been filled and those which remained open.

Further, the lack of integration between ADD and LIMS III hinders FEMA from providing the appropriate number and combination of people and supplies to meet the level of need at disaster locations. Without adequate coordination, personnel might arrive at a disaster site and be unable to begin work because the supplies and equipment they need have not yet arrived, or the supplies may arrive without the necessary people to accept and distribute them. Generally, to achieve the right mix, FEMA's Emergency Operations Center staff laboriously searches through ADD to identify available personnel. Likewise, the Agency Logistics Center must search through LIMS III to identify available supplies. This approach was not effective during the Florida hurricanes when 600 to 800 tractor-trailer trucks of supplies arrived at one staging area within a 24-to-36-hour period. There were only five people at the staging area to accept the supplies because their arrival had not been effectively coordinated with personnel deployments. The truck drivers were forced to wait at the staging area for hours until the goods could be unloaded and processed, a costly delay which hampered disaster assistance.

IT officials agree that it is essential to integrate systems to better support mission requirements, and that this decision must be made in collaboration with the systems owners and program officials. For example, in response to our report, the CIO acknowledged the need to upgrade and integrate IFMIS and FEMA's deployment systems. Systems integration also should consider DHS-wide direction and programs, such as *eMerge*^{2} and *MAX*^{HR}.

State Stakeholders Request Better System Links

Office of Management and Budget Circular A-130 requires that federal agencies integrate state and local government requirements with their information resource management strategies. However, EP&R response and recovery systems do not share information with those used by major stakeholders in state governments. States receiving disaster assistance need to maintain accountability for the federal support they receive. Financial

information, such as the amount of funds allocated, obligated, and expended on behalf of the states is available in NEMIS. While NEMIS' predecessor system did not provide adequate access or internal management controls, it enabled state users to access the FEMA system directly from their desktops. Some states even created automated ways to transfer FEMA information to their state systems. However, this is no longer possible with NEMIS due to security requirements that limit state employees' ability to access NEMIS from their desktops.

Currently, state users can access NEMIS, but not directly from their desktops. Instead, states rely upon stand-alone computers and use manual or convoluted processes to transfer NEMIS information to their state systems. For example, one state uses five stand-alone computers to access NEMIS via a virtual private network, which provides a secure, encrypted connection through the public internet. Users in this state manually re-key NEMIS information into their state systems. Alternatively, they bypass the virtual private network by emailing NEMIS information from the stand-alones to their desktops and then copy the information into the state systems. One user even sent NEMIS information to a home email address. Both such practices create information security concerns.

IT Systems Could More Effectively Support Operations

Because of the unintegrated IT environment, during the 2004 hurricanes, EP&R systems did not effectively handle increased workloads, were not adaptable to change, and lacked needed capabilities. Accordingly, FEMA field personnel developed manual workarounds, adjusted processes, and created alternative IT methods to supplement existing response and recovery systems and operations. Consequently, this created operational inefficiencies and hindered the delivery of essential disaster response and recovery services.

Systems Experienced Difficulty Handling Increased Workloads

FEMA systems were unable to handle effectively the significantly increased workloads required to support disaster victim application processing during the 2004 hurricanes. According to FEMA personnel, they lacked email server space to accommodate messages and reports sent from state and local emergency centers. If someone did not routinely clear the emails from the server, its capacity would fill up—sometimes as much as five to ten times per day—and the system could crash. At one point, the system was down for two hours at the height of the Florida disasters. Workers could not save or download documents. Rather than expand server capacity to resolve the

problem, all workers had to log off of the email server while someone moved emails from the queue file by file.

Further, the surge of disaster victim registrations resulting from the Florida hurricanes overloaded NEMIS' main server, pushing the system beyond its limit. Originally designed to handle a maximum of 20,000 disaster victim registrations a day, during a four-month period from August to December 2004, NEMIS registrations far exceeded these limits during peak periods, reaching over 40,000 on some days. The total number of disaster victim registrations processed during the four-month period of the Florida hurricanes was 1,745,183. The volume of transactions and the number of personnel managing these registrations significantly slowed down the system or made it unavailable for use during peak operations.

Although EP&R CIO staff worked to keep the system operational by increasing system memory, NEMIS' main server became overloaded, the system froze, and unplanned system restarts were necessary. Users were unable to perform their jobs in the system and consequently reverted to paper-based methods. When NEMIS' main server went down, approximately 2,000 IT users were kicked out of the system for as long as 20 to 30 minutes at a time. FEMA personnel accepting victim registrations had to record the information manually and wait to register the victims in NEMIS when the system was functional again. Additionally, FEMA personnel lacked the up-to-date NEMIS information needed to answer disaster victim inquiries when they called the National Processing Service Center for assistance.

As part of our review, we requested system performance reports from the EP&R CIO's office to determine how the systems performed during the hurricane response. However, the CIO office did not have a standard process in place to produce system performance reports. Instead, it had to complete a manual analysis of raw data to provide performance data for only one of NEMIS' key servers. The CIO office stated that it would take several months to supply performance information for all of the other servers. Although the CIO office can monitor central processing unit and hard drive space availability on a real-time basis, it does not have a tool that can show system performance over time. Without such a tool, it is difficult for FEMA to identify system performance problems and take corrective actions to address them.

Given the problems experienced during the 2004 hurricane response and recovery season, a number of FEMA officials expressed concern about not only NEMIS' current capabilities, but also its capacity to support future

dramatic increases in workload. Even the engineers responsible for designing and developing NEMIS questioned whether the system could consistently manage workloads resulting from multiple, concurrent disasters. Although the Florida hurricanes entailed one of the largest response and recovery efforts in FEMA's history, workload volumes from multiple, large disasters in the future could far exceed the systems processing levels required to manage the 2004 incidents.

Systems Are Old and Not Adaptable to Change

FEMA's response and recovery applications are custom designed, complex, outdated, and difficult to adapt to changing user needs. As a result, during disaster response and recovery operations, FEMA has had to adjust its processes to overcome the systems limitations. For example, ADD was designed in such a manner that it cannot be easily updated. Currently, it is difficult to enter into ADD the financial information necessary to issue credit cards, commonly known as "supercards," for emergency response personnel. As a result, FEMA officials created separate, stand-alone databases to track the financial information rather than submit their ADD change requirements to the CIO's office for implementation.

Further, the mail-processing center at the National Processing Service Center in Hyattsville, Maryland, was unable to handle the surge in letter production required during the Florida hurricanes. FEMA employees select and print batches of letters to the victims, categorized by different disaster situations. However, this process became difficult during the 2004 hurricanes because of the increased volume of letters that had to be prepared. No provision had been made for surge printing capability.

CIO officials worked to address the letter generation problem. After 7 to 10 days of effort, they succeeded in improving the system code, helping to reduce the print backlog. However, a contractor later examined the system code and found it to be extremely complex, requiring 20 pages of code to print what newer, more efficient code can do in one line. The contractor recommended rewriting the code; the NEMIS development team currently is investigating ways to address this issue.

In addition to revising the system code to address the print backlog, FEMA changed the business process, instituting a workaround that involved creating one standard letter to send to all disaster victims. The standard letter helped speed up the victim notification process. However, the letter was too generic, did not provide victims the information they needed, and did not clearly

specify what assistance they could expect from FEMA and when it might be available. Confused, the victims called National Processing Service Center representatives for clarification. This created additional burdens as the Center was already overloaded with increased workloads, high call volumes, and slow and crashing systems.

Reporting Challenges

Response and recovery program personnel said that some FEMA systems did not provide useful reports regarding ongoing operations. They said that the standard reports that NEMIS and IFMIS generated were long and did not contain specific information, in the right format, to meet their needs. For example, when a grant report is requested from IFMIS, the product includes all grants instead of identifying specific grant information. Because the reports provided were not useful, FEMA regional offices copied data from the systems and loaded it into spreadsheets and databases so that they could create their own reports. The spreadsheets and databases were not standardized across all regional offices, were not connected with the response and recovery systems, and were not centrally backed up. As a result, regional offices did not maintain consistent information that could be rolled up to the national level.

In addition, requested reports were not timely. At one point in the Florida operations, Individual Assistance Program personnel received a report six days after it had been requested. As a result, 200-300 disaster assistance employees were hindered in their efforts to assist more than 200,000 disaster victims who had requested temporary housing assistance. Without the reports to provide the names and contact information of eligible victims, FEMA was delayed in locating victims to deliver assistance. Other system users said that IFMIS reports take so long to run that they regularly leave the system on over night to produce them. Alternatively, users copy system information, such as financial transaction data, mission assignments, vendor information, and action tracking request forms, onto spreadsheets or databases to access and manipulate the needed data more easily.

Real-Time Resource Tracking Issues

During the 2004 hurricanes, FEMA systems did not provide staff with real-time capabilities for tracking deployments of personnel, equipment, and supplies. For example, ADD did not allow FEMA regional staff to keep track of emergency response personnel sent out to provide assistance at disaster locations. Although ADD contained much of the personnel deployment

information, it did not provide a consolidated view so that regional staff could determine:

- Who had been deployed to the disaster sites;
- Who was en route, but had not yet arrived;
- Who had been sent by FEMA headquarters, but had not been entered into ADD; and,
- Who had arrived at the disaster sites and whether or not they had checked in with the region.

To gain a complete picture of where people were during the hurricanes, the regional deployment coordinator developed a custom database that contained all of the information available and used it to prepare daily reports. Although the reports tracked the "daily" status of people, they did not provide real-time information, potentially placing emergency personnel at risk. For example, when FEMA ordered an emergency evacuation of Orlando, Florida, its regional staff could not obtain from ADD an up-to-date list of deployed personnel and their exact locations. Regional staff had 11 hours in which to manually compile the information, and identify and contact the approximately 200 response and recovery personnel deployed to that area. Fortunately, in this instance, the evacuation was successful. However, the ability to track deployed personnel on a real-time basis is a critical factor to ensuring personnel safety, especially during catastrophic events. According to FEMA officials, the Response Division, which is responsible for ADD, is in the process of developing a replacement for the deployment system.

FEMA cannot use LIMS III for real-time tracking of emergency equipment and supplies deployed to disaster sites. LIMS III is essentially an inventory system used to manage equipment and accountable property, such as cell phones or pagers. LIMS III contains information on the number of items available and where they are located. However, once the items are identified for deployment, LIMS III does not indicate when they will be shipped and when they should arrive. To compensate, emergency personnel in Florida said that they tracked items on a spreadsheet and spent a significant amount of time calling trucking companies to determine the status and projected arrival times of in-transit goods.

Further, LIMS III does not effectively track the exact location of equipment and supplies after they have been issued. FEMA officials said that they do not use LIMS III to issue accountable property during emergency situations, because it takes too long. For example, although accountability property officers made electronic records in LIMS III of bulk goods received during the

Florida hurricanes, these officials used hand receipts to distribute quickly the property to those who needed it. Typically, these transactions were not entered into LIMS III until as many as ten days later, so the system did not maintain an accurate, real-time inventory of the property on hand. Similarly, when Florida requested 500 cell phones, the phones were issued using hand receipts—not through LIMS III. FEMA officials said that it later required about ten minutes to enter the information from the hand receipts into LIMS III for each of the phones issued.

In addition, LIMS III does not track critically needed commodities, such as water, ice, or tarps. Instead, emergency coordinators use spreadsheets to track these goods outside of LIMS III. An Atlanta regional official said that this significantly increased the workload of the regional operations center. This also required the assignment of additional personnel to obtain the status of deployed commodities and complicated emergency response planning and coordination.

For example, during the 2004 hurricanes, the State of Florida requested ice and water via action request forms. Hard copy mission assignments were completed, and the regional operations center used them to assign the request to the U.S. Army Corps of Engineers. The regional operations center tracked the mission assignments via spreadsheets because FEMA does not have a system to track deployed commodities. When asked about delivery status, U.S. Army Corps of Engineers officials could only tell center officials that they were en route with the items. After the items were received onsite, an accountability property officer faxed copies of the paper receipts to the center. This was a time consuming and resource intensive process. In one instance, approximately 1,500 tractor-trailers delivered commodities to a staging area. (See Figure 9). The accountability property officer had to survey the area, manually inventory the commodities received, and email that inventory information to the regional operations center. Because there was no automated way to coordinate quantities of commodities with the people available to accept and distribute them, millions of dollars worth of ice was left unused at staging areas in Florida; and, about $1.6 million worth of leftover water had to be returned to the warehouse for storage.

Figure 9: Tractor Trailers Pick Up Supplies For Disaster Victims

FEMA officials said that they are currently pilot-testing a Total Asset Visibility System to track shipment and distribution of essential commodities such as ice, water, and food. Such a tracking system should provide FEMA with the capability to track assets real-time, across federal, state, and local organizations.

Management Practices Contribute to Systems Operations Problems

FEMA's disaster response culture has supported the agency through many crisis situations, such as the 2004 hurricanes. However, its reactive approach encourages short-term systems fixes rather than long-term solutions, contributing to the difficulties that FEMA encounters in efficiently and effectively supporting response and recovery operations. Without taking the time to fully define and document systems requirements, it is difficult for FEMA to evaluate effectively viable alternatives to its custom designed systems. Further, the reactive manner in which IT systems are funded and implemented has left little time for proper systems testing before they are deployed.

NEMIS Requirements Not Consistently Updated

Office of Management and Budget Circular A-11 directs agencies to reduce project risk by involving stakeholders in the design of IT assets. Users can play an important role in helping to define systems requirements to meet

mission needs. FEMA's approach to defining requirements to support development of its principal disaster management system has not been effective, however. When the CIO office began to develop NEMIS in 1995, the office documented a set of system requirements. But, an EP&R CIO official noted that headquarters personnel were usually responsible for the requirements definition process and that not all of FEMA's stakeholders were involved. Consequently, once NEMIS became operational, the system automated a process that did not reflect how FEMA personnel actually behave during disasters. To address this disparity, the EP&R CIO office had users come in after the initial release of NEMIS to look at each individual module and suggest system changes.

Lacking an effective means to provide input to NEMIS development, users have been forced to rely on systems that do not effectively meet their requirements, modify their processes, or resort to manual workarounds. For example, after an incident occurs, regional officials are supposed to use NEMIS' preliminary damage assessment module to evaluate destruction and losses due to disasters, and subsequently submit that information to headquarters, along with state requests for federal assistance. However, a regional official said that emergency personnel do not use this module to the fullest extent possible. Instead of directly entering the damage assessments into the system, emergency personnel collect and fax the information for review and consideration. The official said that it is easier and faster to submit the damage assessments in hard copy than use the poorly designed NEMIS module.

The EP&R CIO now recognizes the need to improve efforts to reach out to IT users across the directorate and has established forums for discussing and defining system requirements. For example, the EP&R CIO office has assigned each system a customer advocate and a program manager from the various program areas. Program officials approve the requests for systems changes and provide them to IT personnel for further review. IT personnel then discuss how proposed systems changes will be implemented. A policy steering committee, consisting of managers from FEMA headquarters, defines the business processes that are echoed in the technical systems requirements.

Further, the EP&R CIO has proposed updating NEMIS requirements to support the proposed eNEMIS initiative. In commenting on this report, the EP&R CIO discussed plans to elicit broad stakeholder participation in the requirements definition process for the e-NEMIS initiative. Broad stakeholder participation in the requirements definition process will be essential to deliver a web-based NEMIS to meet varied user needs.

However, FEMA officials have not maintained a record of changes to systems requirements nor have they developed an up-to-date NEMIS requirements document. One EP&R CIO staffer said that they have limited funding; when the budget gets pressed, it is always the "overhead" or administrative activities, such as updating requirements documentation, which are bypassed.

Alternatives Analysis Needed

Office of Management and Budget Circular A-130 encourages agencies to consider various options for providing automated systems to meet their mission needs. However, by not taking the time to fully define and document systems requirements, it has been difficult for FEMA to evaluate viable alternatives to the highly complex, custom designed systems that it relies upon to support disaster response and recovery operations. Because these systems have carried FEMA through its responsibilities over the years, senior IT officials said that they have made little effort to evaluate off-the-shelf products to determine if there is a simpler, commercially available, and possibly more effective IT alternative. FEMA's Business Year 2006 business case submission to the Office of Management and Budget for NEMIS improvements also indicates a lack of alternatives analysis.

Members of the EP&R CIO office speculated that off-the-shelf products would likely not meet their needs during peak emergency operations. For example, according to a recent business case for the next generation of NEMIS, there is no plan to perform an analysis of alternative off-the-shelf products or other department systems. The NEMIS requirements document is not up-to-date, and user input to those requirements has been limited. NEMIS is a tool that stretches across multiple business functions; only by having a complete set of documented system requirements for each of these functions will the EP&R CIO be able to determine if alternative products can or cannot fulfill requirements.

In addition, officials in one state agency increasingly have become aware that the federal government cannot compete with the private industry on developing systems. According to this state agency, private industry is developing multiple systems to support emergency management operations. However, because federal systems do not always use the most up-to-date technology, it is becoming more difficult for state agencies to share information with the custom designed federal systems as states upgrade their own off-the-shelf systems.

Lastly, some users said that if FEMA had adopted an off-the-shelf product instead of NEMIS, it would have the additional functions that they need. For example, multiple off-the-shelf enterprise resource planning systems developed by the private sector could possibly support coordination of response and recovery activities. Once FEMA has completely defined all business requirements, it will be in a better position to evaluate available commercial products.

Reactive IT Implementation to Meet Expedited Requests

Federal regulations require that agencies plan in an integrated manner for managing IT throughout its life cycle. However, EP&R's tendency to rush systems acquisition to meet immediate needs has encouraged ad hoc development and implementation of IT programs, which has contributed to many systems integration and performance problems. The EP&R CIO budget in FY 2004 was approximately $80 million. About 90 percent of that amount was earmarked for operating and maintaining existing systems, leaving only 10 percent for new IT initiatives. Consequently, the CIO is dependent on the program offices for any new systems funding.

EP&R has documented plans which propose initiatives and priorities for strategic implementation of long-term IT solutions. However, the program offices in many cases are the owners of the systems, typically do not fund the long-term strategic IT initiatives, and take a cursory approach to short-term systems acquisition. They often do not authorize or fund IT initiatives until disasters occur and specific systems needs become critical. The CIO is working to implement a process for reviewing and approving capital investments—including IT investments—to prevent this from repeating. Until this process is fully implemented, however, the CIO has no means of ensuring that IT investments are well-integrated or aligned with mission needs.

For example, nine months prior to the 2004 hurricanes, FEMA's recovery program offices provided funding to develop and implement an online registration capability for NEMIS. The online system is to allow disaster victims to submit claims via the internet without having to call the National Processing Service Centers. When the 2004 hurricanes occurred, the number of disaster victims registering for assistance increased significantly, thus overloading systems and staff of the National Processing Service Centers. The EP&R CIO was able to deploy the online registration system a full three months earlier than initially planned. However, an EP&R CIO official involved in development of the online systems said that its implementation did not follow standard change management or configuration management

processes. Failing to follow such processes ultimately leads to systems availability problems. The Gartner Group, a leading provider of IT industry research and analysis, reported that 80 percent of unplanned systems downtime is caused by people and process issues, including poor change management practices. Enterprises which have established strong change management practices typically have the highest levels of systems availability.[19]

Additionally, according to regulations, agencies are responsible for ensuring effective and efficient operation of IT equipment before it is implemented. This entails proving that new systems function in a "production-like" test environment to ensure that the IT applications work properly and contain needed safeguards. However, in addition to its rushed systems acquisition approach, the EP&R CIO does not have a test environment to match the real systems environment, and does not always adequately test systems prior to release.

For example, the online NEMIS registration capability did not have a name check function to ensure the validity and existence of the individuals filing claims. Also, the online system did not have controls to prevent one individual from generating multiple claims at the same time, even though the technology to prevent this from occurring already exists. One FEMA official was aware of six false claims made online. Proper testing of the online system likely would have disclosed this lack of system controls, leaving FEMA less susceptible to such fraud. FEMA officials said that they are in the process of acquiring the identity proofing, authentication, and prevention capabilities needed to mitigate these risks.

Further, a FEMA testing team lacked adequate requirements to support testing of a new fire grants system. When it updated the production environment with the new system code, the system automatically sent multiple print jobs across the network, clogging up the system, and taking bandwidth away from emergency personnel who needed it.

[19] *NSM: Often the Weakest Link in Business Availability*, Gartner, Inc., July 3, 2001.

Recommendations

We recommend that, in keeping with legislative requirements, the Under Secretary for EP&R:

3. Direct the EP&R CIO to complete the FEMA enterprise architecture, linked to the departmentwide architecture and ongoing initiatives that may impact EP&R operations.

4. Ensure cross-cutting participation from headquarters, regions, and states in processes to develop and maintain a complete, documented set of FEMA business and system requirements. Direct the EP&R CIO to analyze alternatives and determine the most appropriate approach to providing the technology needed to support these business and system requirements.

5. Direct the EP&R CIO to develop and maintain a testing environment that duplicates the real systems environment and ensures that all systems components are properly and thoroughly tested prior to their release. Additionally, direct the EP&R CIO to ensure that proper configuration management activities are followed and documented.

Management Comments and OIG Evaluation

We obtained written comments on a draft of this report from the Chief Information Officer (CIO), Emergency Preparedness and Response (EP&R), through the EP&R Under Secretary. We have included a copy of the comments in their entirety at Appendix B.

In the comments, the EP&R CIO found the draft report to be unacceptable, stating that it incorrectly characterized FEMA's strategic planning and IT activities and needed to be revised. The EP&R CIO also said that the overall tone of the report was negative and did not acknowledge FEMA's "highly performing, well managed, and staffed IT systems," leading the reader to conclude that EP&R is lacking, particularly in the areas we cover in our report recommendations. The EP&R CIO invited us to meet with FEMA's strategic planning unit to best judge the extent to which the agency is in line with DHS strategic direction, as well as meet with EP&R CIO officials to clear up some of what the CIO called "obvious inaccuracies."

We do not agree with the EP&R CIO's response. First, it should be noted that during the audit we met with FEMA's strategic planning unit, as well as with other program officials to discuss the agency's planning activities. Based on these meetings and our review of supporting documentation, we devised findings and recommendations regarding the need to update the strategic plan and establish better linkages between it and the IT plan. At the May 17, 2005, audit exit meeting where we discussed a preliminary draft of the report, EP&R CIO officials did not address our conclusions or recommendations regarding strategic planning. Indeed, one FEMA official conceded that the lack of alignment in strategic planning likely was due to creation of the EP&R directorate and FEMA's transition into the department—events over which they had little control.

Second, with regard to the EP&R CIO's concern about the overall tone of the report, we made considerable efforts to revise the report based on comments that EP&R CIO officials provided during our audit exit meeting and their review of a preliminary draft of our report pursuant to that meeting. In response to the EP&R CIO's formal written comments, we have assessed the tone of the report and made additional changes where appropriate. Still, a number of the IT issues we raise, such as the lack of systems integration and challenges in handling processing workloads, are not new, dating back to well before the current EP&R administration and FEMA's integration into DHS, and were consistently evidenced or voiced to us by EP&R officials and systems stakeholders during our audit. We acknowledge in the report the various instances where EP&R is working to address such issues; our recommendations are intended to encourage continued progress and improvement in these areas.

Third, we believe that the EP&R CIO incorrectly equates the agency's ability to meet the disaster management challenges to date with effective and efficient IT management. While we state in our report that EP&R was able to get through the 2004 hurricanes, often experiencing significant achievements, high customer satisfaction, and high volume processing, we also recognize that FEMA's accomplishments were not necessarily because of its IT systems, but often in spite of them. Users across EP&R consistently told us that they did not use the headquarters-supplied systems, but instead relied upon alternative methods, such as creating ad hoc spreadsheets and databases or resorting to manual methods, to perform their jobs. Where IT systems were used, they often did not operate effectively. For example, systems were slow, froze, or lacked server space or memory due to the dramatic increases in systems users and processing workloads during the 2004 hurricanes. The EP&R CIO's own FY 2005 strategic plan also states that during the

hurricanes, "both NEMIS and its support staff were stressed to the limit and that Herculean efforts were required to meet demands that exceeded several design requirements by an order of magnitude." The tremendous effort required to meet the 2004 challenges logically evokes questions about the ability of FEMA's IT systems to prevail in supporting future disasters. Indeed, senior officials and a lead engineer for one of FEMA's primary systems repeatedly shared with us concerns about the system's ability to withstand potential multiple or catastrophic events.

Fourth, given the IT issues expressed above, we believe that the EP&R CIO is not justified in referring to EP&R's "highly performing, well managed and staffed IT systems" and that our overall message that IT could be better managed is warranted. Though the EP&R CIO suggested in his comments that a review with him, "may clear up some of the obvious inaccuracies," it should be pointed out that we maintained ongoing communications with the EP&R CIO's office during the course of our audit. For example, as requested, we met on a monthly basis with the EP&R CIO, or representative staff when the EP&R CIO was unavailable, to discuss audit progress, IT issues, and potential findings. In addition, as discussed previously, we held an audit exit meeting with the EP&R CIO and key IT officials, providing, as a courtesy, the opportunity to submit informal comments on a preliminary draft of our report, which served as input to the draft subsequently distributed for formal written comments.

The EP&R CIO neither concurred nor non-concurred with our recommendations, but instead provided additional detailed comments and information to update or supplement issues we outline in our report. The following discussion provides our evaluation of each of the EP&R CIO's additional comments.

FEMA's Support for DHS Strategic Goals: The EP&R CIO provided a number of comments on our treatment of FEMA strategic planning issues, and these are discussed below:

- We disagree with the EP&R CIO's statement that our conclusion that "FEMA does not support DHS' strategic goals" is based on what the CIO calls a "misunderstanding of the relationship between FEMA's plans and metrics, and those of DHS." Our audit did not seek to analyze comprehensively FEMA's strategic planning processes. Rather, our objective was to review EP&R's approach for responding to and recovering from incidents. In this context, we examined the strategic and IT plans in place to determine whether they are appropriately linked to

support an alignment between DHS, FEMA, and response and recovery IT initiatives. Our review showed clear disconnects among the planning documents. Specifically, FEMA's strategic plan was created prior to the agency becoming part of DHS, has not been updated since then, and consequently does not align with specific response and recovery metrics outlined in DHS' plan. We reviewed FEMA's IT strategic plan to determine whether technology approaches and initiatives support response and recovery mission goals and found that the IT plan is based on FEMA's outdated strategic plan. As such, we recommended that both FEMA's strategic and IT plans be updated.

- Contrary to the EP&R CIO's statement, we neither assume nor state in our report that FEMA's strategic plan is the only mechanism to ensure alignment of FEMA plans and programs with DHS goals and objectives. As stated above, we focused on FEMA's strategic plan, because the EP&R CIO office identified this plan as the basis for IT planning and direction. Further, according to the *Government Performance and Results Act of 1993*, performance-based management and budgeting must begin with an overarching strategic plan. As a result of our review, we identified misalignments between DHS' and FEMA's strategic planning documents that we would be remiss in not discussing in our report. We did not seek to analyze FEMA's overall strategic planning process, or any of the other planning, programming, budgeting, and execution processes that the EP&R CIO identified. Such processes were outside of the scope of our audit.

- We neither dispute nor discuss the EP&R CIO's assertion that the goals and metrics identified in DHS' strategic plan were written by FEMA. Again, our intent was to point out disconnects between DHS' and FEMA's strategic planning documents and the need for FEMA updates to better support IT planning. Nonetheless, we have revised our report to state that FEMA not only participated in working groups to help develop the DHS plan, but also defined and owns the response and recovery goals and metrics outlined in the DHS plan.

- We believe that the EP&R CIO's statement that some information in FEMA's strategic plan has been outpaced by events helps support our argument that the plan is outdated and needs to be revised. Even though the main body of FEMA's strategic plan may remain applicable since the agency has become part of DHS, updating the plan as we recommend will help ensure that the FEMA and DHS plans do not conflict, but also support each other. We have revised the language in our report to clarify

our concern that use of the two plans as they currently exist could lead to ambiguous guidance and direction.

- We agree with the EP&R CIO's statement that FEMA came into the department as a whole and that its mission was not dramatically altered, although the transition into DHS brought a new focus to the agency's activities. Our report does not contest the continuity of FEMA's all-hazard response and recovery mission in the context of the new department. Rather, our report recommends that FEMA update its strategic plan to reflect this organizational realignment, support achievement of DHS goals, and provide updated guidance on which to base IT planning.

- We believe that FEMA's acknowledgement that it postponed a review of its strategic plan due to the demands of the 2004 hurricane season supports our argument that the plan is outdated and needs to be revised. We stand by our assertion that the plan is outdated, however, not from a calendar standpoint, but rather in the sense that it does not align with DHS' plan and reflect FEMA's integration into the new department. We recognize in our report that the schedule for updating the plan has been postponed due to events such as the 2004 hurricanes. Recommendation 1 is intended to encourage FEMA to proceed in updating the plan so that the document may serve as a useful and current guide to support IT planning.

FEMA's Participation in DHS Strategic and Performance Planning: We accept FEMA's suggestion that we revise our report to reflect the relationship between FEMA and DHS in establishing performance goals and metrics. As previously stated, we have revised our report to indicate that FEMA not only participated in working groups to help develop the DHS plan, but also defined and owns the response and recovery goals and metrics outlined in the DHS plan.

OMB Guidance on Linking Department and Component Plans: We disagree with the EP&R CIO's statement that the report incorrectly cites OMB Circular A-11 as guidance for agencies to create their own strategic plans linked to overarching departmentwide plans. Section 210 of Circular A-11 states that an agency's strategic plan provides an overarching framework, keying on those programs and activities that carry out the agency's mission. The circular states that although a single plan should be submitted, the *Results Act* allows an agency with widely disparate functions to prepare several strategic plans for its major components or programs. In these instances, an overview that brings together the component plans is prepared. In line with these

requirements, DHS' strategic plan constitutes a single framework for consolidating the missions, goals, and objectives of its 22 agencies in a joint strategy for securing the homeland. As one of the legacy agencies, FEMA's strategic plan necessarily should link to the overarching DHS plan. We have revised our report to clarify these requirements.

Conflicting Guidance and Direction: We agree with the EP&R CIO regarding the potential for misconstruing our statement that a planning official's use of both DHS' and FEMA's strategic plans results in conflicting guidance and direction. We have revised this language to show that the potential for conflicting guidance and direction is our conclusion, and not attributable to the planning official. We also have revised the wording in the relevant section of the report to ensure consistency with our executive summary.

IT Strategic Plan Alignment with the DHS Plan: Contrary to the EP&R CIO's assertion, our report neither contests nor discusses alignment of FEMA's IT strategic plan with DHS CIO Council priorities. While we commend FEMA's cooperation with the CIO Council, we did not include this issue in our audit. The strategic planning portion of our report is merely intended to emphasize that, despite federal guidelines, FEMA has not aligned its strategic and IT plans with the overarching DHS strategic plan.

Handling Workloads during the 2004 Hurricane Season: We disagree with the EP&R CIO's assertion that FEMA would not have been able to successfully handle the increased workload during the 2004 hurricane season if the agency were experiencing the various IT problems that we outlined. As previously indicated, we believe that the EP&R CIO incorrectly equates the agency's ability to meet the disaster management challenges to date with effective and efficient IT management. While we state in our report that EP&R was able to get through the 2004 hurricanes, we also recognize that FEMA's accomplishments were not necessarily because of its IT systems, but often in spite of them. Users across EP&R consistently told us that they did not use the headquarters-supplied systems, but instead relied upon alternative methods, such as creating ad hoc spreadsheets and databases or resorting to manual methods, to perform their jobs. Where IT systems were used, they often did not operate effectively.

Enterprise Architecture: We disagree with the EP&R CIO's assertion that we incorrectly reported on EP&R efforts to update its enterprise architecture to govern the IT environment. The following is our evaluation of the EP&R CIO's various comments in this regard.

- First, we do not agree that our discussion of enterprise architecture issues in the executive summary of our report is misleading. The purpose of the executive summary is to bring together the various parts of our report to comprise an overall message. We believe that completing an enterprise architecture is important to provide a framework for ensuring effective systems integration, functionality, and information sharing, unlike what was experienced during the 2004 hurricanes.

- Second, we appreciate the EP&R CIO's concern that our discussion of the status of enterprise architecture development is based on out-of-date information. We based our statement that the electronic "as is" enterprise architecture was approximately 85 percent complete and that the "to be" architecture development had not yet begun on discussions with the lead enterprise architecture official, held as recently as June 2005. We acknowledge the range of ongoing activities to further progress in architecture development and have revised our report to reflect these efforts. However, although the EP&R CIO cites such activities, the EP&R CIO does not provide an up-to-date, quantifiable indication of the current status of architecture development, as compared with the October 2005 target completion date. Based on the information provided to date, our recommendation remains to proceed with architecture development and make it available as a framework for guiding FEMA's IT management in line with the DHS architecture and ongoing initiatives.

- Third, we disagree with the EP&R CIO's comment that our report assumes that the incomplete enterprise architecture alone is the reason for IT systems not efficiently handling increased workloads. The EP&R CIO has taken our reference to the enterprise architecture out of context and misconstrues the issue that we raise. Rather, we conclude in the executive summary of our report that the incomplete enterprise architecture, in conjunction with unintegrated systems and ineffective information exchange, creates an ineffective processing environment.

- Fourth, we have revised our report to reflect the EP&R CIO's comments regarding recent progress in developing the "as is" and "to be" portions of FEMA's enterprise architecture. We recognize that overall architecture development is an evolving process, but nonetheless encourage FEMA to complete the "to be" portion to serve as a roadmap for proposed IT initiatives.

EP&R CIO Budget: We agree with the EP&R CIO there is a potential to misconstrue our statement regarding the resources used to develop and operate

IT for response and recovery. We have revised our report to reflect more accurately the activities performed by EP&R CIO personnel.

LIMS III: As the EP&R CIO suggested, we have updated our report to refer to the Logistics Information Management System as LIMS III, not LIMS. Although we evaluated how effectively LIMS III supports the logistics management process, we did not follow up and report on recommendations from prior audits regarding logistics data accuracy.

Prior GAO and OIG Assessments: We disagree with the EP&R CIO's statement that our references to past OIG reports, without referring to the current status of these reports, may give an inaccurate and unfair picture of IT status. We referenced prior GAO and OIG assessments only to provide background information and a context for conducting our audit. While the scope of our review did not include following up on all findings and recommendations from these prior assessments, it should be recognized that many of the concerns they raised, such as NEMIS reliability, usability, and training, remain issues today.

ADD Functionality: We recognize that the Automated Deployment Database has a "check-in" process and a date/time stamp for when personnel call headquarters to advise of their arrivals at disaster sites. However, as we discuss in our report, personnel do not always follow the prescribed check-in procedures and information on their arrivals may not be entered into ADD to measure deployment time. Inconsistent check-in not only affects the accuracy of ADD reports, but also may leave response and recovery personnel at risk when their whereabouts are unknown.

LIMS III Tracking: We recognize, as the EP&R CIO has indicated, that LIMS III was not designed to track commodities such as ice and water. We are concerned that the lack of a system or a formal requirement to track such commodities not only does not meet requirements of the National Incident Management System, but also creates problems for response and recovery personnel. As we discuss in our report, property officers must resort to spreadsheets, manual processes, or other inconsistent and nonintegrated means to track commodities, resulting in wasted time, effort, and resources. We encourage FEMA's ongoing efforts to develop a total asset visibility system to track commodities and expect that such a system will provide FEMA with improved ability to track and measure distribution of assets across federal, state, and local agencies.

Response and Recovery Performance Metrics: We agree that EP&R systems are not entirely owned by the CIO's office and recognize that the program offices, which are the systems users, also need to help identify effective performance measures. The EP&R CIO's comments affirm the need for improved ability to collect performance data from IT systems. Recommendation 1 of our report addresses the need for improved performance measurement.

Departmentwide Initiatives: The additional information that the EP&R CIO provided on FEMA's efforts to coordinate its IT activities with departmentwide initiatives affirms issues and recommendations we raise in our report. Where appropriate, we have revised the report to reflect the ongoing coordination activities.

IT Guidance and Training: Again, the EP&R CIO's comments affirm and supplement the information we provided on IT guidance and training in our report. Like the EP&R CIO, we expect that having regional IT staff report directly to his office will enhance efforts to define training requirements, integrate and improve training materials, and better communicate guidance and training availability.

Database Integration: The EP&R CIO commented that our discussion under the report heading "Databases Are Not Fully Integrated" should be omitted because it is not relevant to either database integration or mission application integration. In response, we have revised the heading and clarified the subsequent discussion concerning the need to centralize NEMIS servers.

Logistics Integration: The EP&R CIO stated that our example regarding logistics coordination is partially incorrect in that not all of the tractor trailers came from the FEMA Logistics Centers. Our report does not say that all of the trucks came from the FEMA logistics center. Indeed, where the trucks came from is not germane to the issue that we raise. Rather, we are concerned that, although FEMA is responsible for coordinating federal incident response, the arrival of all of the trucks at a single staging area was uncoordinated and personnel were not on hand to receive the supplies in a timely manner.

NEMIS Access and Security: We recognize that cyber security requirements limit the ability of state employees to access NEMIS from their desktops and have revised our report accordingly.

System Capacity to Handle Increased Workload: We disagree with the EP&R CIO's comments regarding the ability of FEMA's IT systems to handle

increased workloads during the 2004 hurricanes. As previously stated, while we recognize that FEMA was able to get through the hurricanes, this accomplishment was not without significant IT and user problems. Like the EP&R CIO, we acknowledge that much of the credit can be attributed to the efforts of IT and recovery staff who worked heroically during the hurricanes to sustain operations and register and assist disaster victims. We also appreciate the EP&R CIO's challenges and lack of resources to carry out operations on a day-to-day basis. However, as we recommend in our report, EP&R needs to place priority on gathering requirements and analyzing alternatives to determine the most appropriate technology needed to meet business needs.

System Reporting: Although the EP&R CIO stated that LIMS III provides substantial reporting capabilities, the cited section of our report discusses NEMIS and IFMIS challenges and does not mention LIMS III. We have revised the topic sentence for the section to indicate reporting challenges with some, but not all, of FEMA's systems.

Need for Updated NEMIS Requirements and Alternative Analysis: The EP&R CIO affirms the responsibility of management at all levels to recognize and act on problems such as the need to update NEMIS requirements and conduct an alternatives analysis. We look forward to the results of the EP&R CIO's efforts to solicit broad stakeholder involvement in the e-NEMIS requirements definition process. Additionally, we have revised our report to incorporate the EP&R CIO's acknowledgement of the need to integrate and update systems such as IFMIS and FEMA's deployment systems.

Funding for NEMIS Upgrade: In response to the EP&R CIO's comment, we have revised our report, deleting the statement that program offices were reluctant to fund development of an online registration capability for NEMIS.

As background for this audit, we researched and reviewed IT laws, regulations, and other federal guidance applicable to the EP&R directorate. We researched and reviewed prior OIG, Government Accountability Office, and other reports relating to EP&R IT to identify relevant findings and recommendations. We also reviewed information available on the DHS and FEMA websites about disaster response and recovery initiatives.

We met with EP&R management officials and staff to review the directorate's approach to responding to and recovering from terrorist attacks, major disasters, and other domestic emergencies. These officials discussed EP&R's organization, roles, responsibilities, operations, and systems for response and recovery activities. Additionally, these officials discussed EP&R's strategic planning process and provided copies of DHS, FEMA, and EP&R CIO strategic, performance, and operational plans. We reviewed the plans to determine alignment of the various organizations' goals, objectives, and performance measures.

We visited EP&R field offices and state government organizations to assess IT user guidance and support. Emergency management officials, IT support staff, and system users at the following locations discussed the effectiveness of EP&R's guidance and processes for responding to and recovering from disaster incidents:

EP&R Headquarters

- CIO officials and IT support staff
- Mt. Weather personnel
- Response Directorate officials
- Recovery Directorate officials

FEMA Regions

- Region II—New York, New York
- Region IV—Atlanta, Georgia
- Region IX—Oakland, California

State Emergency Management Organizations

- New York Public Security Office and New York State Emergency Management Office—Albany, New York
- State Office of Emergency Services—Sacramento, California
- Georgia Emergency Management Agency—Atlanta, Georgia
- Maryland Emergency Management Agency—Reisterstown, Maryland
- State Homeland Security Offices—Albany, New York

These officials, as well as representatives of the following organizations, helped us accomplish our objective of determining how effectively IT systems supported EP&R's response and recovery mission.

National Processing Service Centers
- Hyattsville, Maryland
- Pasadena, California

Disaster Field Offices
- Burlington, New Jersey
- Albany, New York
- Orlando, Florida

Disaster Recovery Center
- Orlando, Florida

Mobile Emergency Response Service
- Thomasville, Georgia

These stakeholders told us about both existing and proposed EP&R systems as well as ad hoc systems they created to meet their needs. Lastly, we met with officials from the *eMerge*^{2} program to discuss EP&R's participation in this effort and to gain a better understanding of what the program will do for DHS.

We limited our audit to EP&R's unclassified systems and processes related to the response and recovery mission, and did not focus on sensitive systems or information. In addition, we did not test the data in the systems reviewed for accuracy and completeness. Throughout the course of this audit, we provided monthly updates to the EP&R CIO on progress and discussed key issues identified by the stakeholders.

We performed our work according to generally accepted government auditing standards. The principal OIG points of contact for this audit are Frank Deffer, Assistant Inspector General, Information Technology Audits and Sondra McCauley, Director, Information Management Division. Other major contributors are listed in Appendix C.

U.S. Department of Homeland Security
Washington, D.C. 20472

FEMA

August 3, 2005

MEMORANDUM FOR: Richard L. Skinner
Acting Inspector General

THROUGH: Michael D. Brown
Under Secretary
Emergency Preparedness and Response

FROM: Barry C. West
Chief Information Officer/Director
Information Technology Services Division

SUBJECT: Audit Report dated June 2005 -
"Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery"

We have reviewed the rewrite of the Audit report and find it unacceptable. The report incorrectly characterizes our Strategic Planning and IT activities. EP&R therefore invites the Office of the Inspector General to meet with the Agency's strategic planning unit to discuss how plans and metrics are developed within FEMA and DHS, and how best to judge the extent to which FEMA is in line with DHS strategic direction. The report erroneously portrays information technology (IT) as poorly managed yet states in the Results in Brief section that "EP&R's IT approach has met the disaster management challenges to date...." The body of the report also contradicts this erroneous portrayal. In the section labeled "IT Support During the Florida Storms" you reported on the significant achievements, high customer satisfaction, and high volume of processing. None of this would have been possible if IT was poorly managed. We suggest a review with our CIO may clear up some of the obvious inaccuracies.

The overall tone of the report is negative, leading the reader to conclude that EP&R is lacking in the areas covered under your recommendations, particularly strategic planning, involvement in DHS-wide initiatives, and progress on the enterprise architecture. We believe this characterization is inaccurate and does not acknowledge the highly performing, well managed and staffed IT systems supporting FEMA incident response and recovery.

In view of these inaccuracies and misrepresentations, we recommend that the report be revised to address the issues presented by EP&R in the attachment. Should you have any questions, please contact Barry C. West at (202) 646-3006.

Attachment

Attachment

Comments on Draft Inspector General Report:
"Emergency Preparedness and Response Could Better Integrate with Incident Response and Recovery."

Now on Page 2

On page 5 the report finds that FEMA "does not support DHS' strategic goals." This conclusion appears to be based on a misunderstanding of the relationship between FEMA's plans and metrics, and those of DHS. FEMA therefore invites the Office of the Inspector General to meet with the Agency's strategic planning unit to discuss how plans and metrics are developed within FEMA and DHS, and how best to judge the extent to which FEMA is in line with DHS strategic direction.

Under Results in Brief, we believe the OIG incorrectly concludes that the IT planning "…does not reflect FEMA's integration into DHS and therefore does not support DHS' strategic goals." The report assumes that the FEMA strategic plan is the only mechanism that ensures alignment of FEMA plans and programs with DHS goals and objectives. In fact, the primary mechanism for ensuring alignment to the Departments goals is the DHS five-year plan and budget: the Future Years Homeland Security Program (FYHSP). Through the Planning, Programming, Budgeting and Execution (PPBE) process that creates and executes the FYHSP, FEMA ensures that DHS goals and objectives are directly supported by the Agency's programs, activities, and budgets.

Now on Pages 6-12

The report reflects a mistaken understanding of the relationship between FEMA's plans and programs, the DHS strategic plan, and the Department's five-year FYHSP. This is demonstrated throughout the discussion on pages 10 through 15. On pages 11 and 12 (*Figure* 3 and *Figure 4*), for example, the report incorrectly portrays the goals and metrics in the FYHSP database as "DHS goals" and "DHS metrics." On page 13, the report states that "in 2004 DHS allotted 72 hours for providing both emergency teams and essential services to disaster areas," explaining, incorrectly, that this "illustrates DHS' performance objectives for FEMA response times."

There is, in fact, no difference between DHS and FEMA metrics. The "DHS" strategic goals and supporting metrics cited in the report were not handed down by the Department, but instead were actually written, and are owned by, FEMA. FEMA reports its progress against these metrics to DHS quarterly, and has aligned its entire budget and activity structure to the DHS strategic plan, and has done so since 2003.

Now on Page 2, 8, 9

The report consistently refers to FEMA's "outdated strategic plan" (refer to Pages 5, 12 and 13). As acknowledged in the audit team's introductory meeting with FEMA's strategic planning unit, some of the information in the FEMA strategic plan has been outpaced by events; FEMA's terrorism preparedness goal, in particular, has continued to evolve since 9/11. For the most part, however, the main body of the plan is still applicable to FEMA's programs and activities. This point was emphasized at the outset

of the audit in FEMA's discussion of the Agency's strategic plan, but is not mentioned in the report. Moreover, as an active participant in the development of the DHS strategic plan, FEMA ensured that the response and recovery goals and objectives in the Agency's strategic plan do not conflict with the Department's plan.

FEMA, in contrast to any other organizational element of DHS, came into the Department as a whole and independent agency. More significantly, FEMA arrived in DHS with a mission that was not dramatically altered. FEMA has always been an all-hazards emergency management agency. Although 9/11 and the Agency's transition into DHS have brought a new focus to FEMA's activities, by virtue of Federal statute, and because natural hazards and other non-terrorist hazards continue to exist, FEMA's mission has remained substantially unchanged.

The report's designation of the FEMA plan as "outdated" might suggest to some that the plan is old. In actuality, the FEMA strategic plan has only been in effect for two fiscal years. It should also be noted that the DHS strategic plan was released just a year ago, in February of 2004. From this perspective the Agency's plan is certainly not "outdated." As stated in the report, FEMA had planned to make any necessary updates to its strategic plan last summer, but the review was postponed because of the demands on FEMA leadership and staff caused by the unusually destructive 2004 hurricane season. An update this year has also been delayed, pending results of the Secretary's Second Stage Review.

Now on Page 7

On page 10 the report states "DHS developed its strategic and performance plan which, taken together, establish its mission and outline goals and metrics for its disaster response and recovery efforts. FEMA participated in working groups to provide input into development of these plans." This passage should be changed to accurately reflect the true relationship between FEMA and DHS in establishing goals and metrics. FEMA was an active participant in the development of the DHS goals and objectives for EP&R and more than just providing input, FEMA in fact developed and owns all of the metrics that support the response and recovery sections of the DHS strategic plan.

Now on Page 7 and 8

On page 11 the report stated "Although Office of Management and Budget Circular A-11 directs that component agencies create their own strategic plans linked to overarching department wide plans…" This statement should be removed or reworded without the reference to A-11. There is no language in OMB Circular A-11 directing departmental components to do this. The latest version of OMB's guidance can be found here: http://www.whitehouse.gov/omb/circulars/a11/current_year/s200.pdf

Now on Page 8

On Page 12 the report states "A planning official said that FEMA uses both the DHS strategic plan and FEMA's outdated plan, which results in conflicting guidance and direction." This statement needs clarification. It could easily be misconstrued as saying a FEMA official stated that the two plans result in "conflicting guidance and direction." This is the IG's conclusion, not the FEMA strategic planning unit's conclusion. The FEMA strategic planning official said only that both plans are in use.

Now on Page 9

Under Results in Brief the report states "while the IT plan aligns with FEMA's outdated strategic plan, it does not reflect FEMA's integration into DHS and therefore *does not* support DHS strategic goals." This language does not match the language in the body of the report. In the *Results of Audit* section (Page 13), the report states: "As a result, the initiatives defined by the CIO organization may *not support* the achievement of the response and recovery goals and metrics established by DHS."

Now on Page 9

On page 12 the report indicates that the initiatives contained in the IT strategic plan do not align completely to goals and metrics identified in DHS level planning. FEMA's Chief Information Officer (CIO) developed the IT strategic plan for FY 05 to address the DHS CIO Council priorities set forth for FY 05, as well as FEMA goals. The DHS CIO Council priorities are:

- Transform the Enterprise – Focus on information sharing to provide the right information to the right people at the right time and provide a roadmap for innovation across DHS while supporting the Department's business and mission objectives.
- Secure the Homeland – Builds on the DHS role as the nation's security flagship by ensuring DHS networks, increasing information security awareness in our employees, and achieving compliance with the Federal Information Security Management Act (FISMA).
- Finish the Foundation – Seeks to establish one enterprise-wide IT infrastructure and maximize its IT investments through a formal portfolio management program.
- Stand Up the Start-ups – Provides mission capabilities and IT infrastructure to those components lacking legacy systems before the establishment of DHS, i.e., the Office of the Secretary, Transportation Security Administration (TSA), the Directorate of Information Analysis and Infrastructure Protection (IAIP), Directorate of Science and Technology (S&T), and the Management Directorate.
- Empower the IT Workforce – Seeks to identify skills gaps in the Department's IT workforce, develop training and recruiting programs, as well as e-Learning capabilities, and the next generation of IT leadership.

The FEMA IT strategic plan for FY 05 defines six strategic management initiatives (SMIs) for the Information Technology Services Division (ITSD) management to achieve the DHS and FEMA priorities. These SMIs are:

- Governance - To transform IT planning and administration from small, independent processes into major departmental processes in a manner that aids integration and performance by FEMA within DHS, and to implement a disciplined capital planning and investment control process Agency-wide. The CIO recognizes the importance of governance to promote understanding, improve

productivity, and reduce costs, and the IT Strategic Plan included goals and objectives to complete the governance documentation and training needed. The combination of good governance and achievement of EA target objectives, will assure FEMA of a completed, IT portfolio in the coming years. Significant improvement to project and program management will also result from this valued combination.

- Next Generation NEMIS - To enhance the existing NEMIS platform, which, as recognized in your report, is currently being stretched almost beyond capacity. The target infrastructure of NEMIS should allow it to support concurrent, multiple, catastrophic disasters and interface seamlessly with the Department since FEMA provides task assignments to other organizational elements, such as the Coast Guard and Border and Transportation Security Directorates. The CIO wants to assure that FEMA can provide the level of information technology support necessary in the event of multiple catastrophic events.

- Enterprise Architecture - To improve communication between FEMA's business and IT senior managers and serve as the official organizational "blueprint" for the capital investment planning process. The EA enables the consistent and disciplined use of technology, reduces stovepipe solutions and redundancies, and provides FEMA with the capability to plan more efficiently by identifying gaps between the existing and future architectures. The CIO directed that the Chief Enterprise Architect move the organization forward from the "As-Is" toward the "To-Be" EA, to improve interoperability and information sharing capabilities across FEMA and the Department.

- IT Security: To educate all Program Managers on the importance of IT security; develop training processes and plans to educate the Business Units on certification and accreditation; and have all FEMA IT systems fully certified and accredited by the end of the fiscal year to achieve the certification requirements established by the National Institute of Standards and Technology (NIST). The CIO set forth goals and objectives to guarantee that our IT resources are available when needed, that our data are appropriately secured, and efforts continue to improve our Information Security Program and ensure that our IT systems are certified and accredited for operations.

- Strategic Partnerships: To enhance IT services by requiring coordination and cooperation between all IT entities in an effort to improve services and gain the confidence and cooperation of customers through developing an operational "human network" for the Office of the CIO. This includes reaching out to peers within FEMA, DHS, and our user community so that the value of IT and the services of the ITSD are clearly understood by all stakeholders. The IT Strategic Plan specified goals to strengthen strategic partnerships to ensure that our partners in the Agency as well as at the DHS understand our capabilities and how to use them to improve operational efficiencies.

- Human Capital: To recruit, train, cross-train, and provide incentives to retain highly skilled staff to support the IT mission. It includes establishing and implementing a succession plan to ensure continuity of knowledge management, critical to ensuring "best practices" are documented, "lessons learned" are passed down, and transition planning is a routine action. The IT Strategic Plan specified goals and objectives to ensure that FEMA has the best-qualified and skilled staff to make the Agency a world-class enterprise.

The SMIs represent important directions and management goals required to satisfy functional, technical and business needs of FEMA's major operating Divisions and Offices and demonstrate that our IT planning is aligned with the DHS direction.

Now on Page 2

On page 5 the report indicates that "…EP&R systems are not integrated and do not effectively support information exchange during response and recovery operations." It goes on to state that "EP&R has not fully updated its enterprise architecture to govern the IT environment," and concludes "As a result, during significant disaster response and recovery operations, such as the 2004 hurricanes, IT systems cannot effectively handle increased workloads, are not adaptable to change, and lack needed real-time reporting capabilities. Such problems usually are due to FEMA's focus on short-term IT fixes rather than long-term solutions. Inadequate requirements definition, alternatives analysis, and testing prior to systems deployment are characteristic of this reactive IT management approach." If this were true, FEMA would not have been able to successfully handle the increased workload during the 2004 hurricane season.

We strongly disagree with the Enterprise Architecture (EA) information presented in the OIG Report. Apparently, the report was based on out-of-date EA data and does not reflect the current status of the FEMA EA or the activities that are being championed by the FEMA Enterprise Architecture Office (EAO). Therefore, the report is misleading, inaccurate and does not reflect the work that has occurred in the past fifteen months.

Now on Page 2

On page 5, it states: "…Also, EP&R has not fully updated its enterprise architecture to govern the IT environment. As a result, during significant disaster response and recovery operations, such as the 2004 hurricanes, IT systems cannot effectively handle increased workloads, are not adaptable to change, and lack needed real-time reporting capabilities…" This statement is NOT true. The FEMA EAO has established an EA web site (online.fema.net/ea). The entire enterprise has access to the EA. The site contains instructions, guidance and other information pertinent to achieving EA objectives. Special web-based Exhibit 300 instructions are also located on the website. These instructions were developed to facilitate Program Managers in completing Section II.A, EA, of the Exhibit 300. As part of the guidance process, the EAO has incorporated EA into the Capital Planning Investment Control Process (CPIC). This process is documented in the EA Governance Manual and is also posted on the EA web site. The Governance Manual provides detailed instructions on processes and procedures. To-date, there has been four releases of the EA web site. In each release, additional content and capabilities are being added.

The EAO has lead efforts to establish a Software Waiver Review Team (SWRT). The SWRT is responsible for reviewing proposed software purchases, validate adherence to the DHS Technical Reference Model or evaluate requests/justifications for waivers. The CIO is the approving authority for the proposed software waiver. The SWRT process is also documented in the EA Governance Manual.

During the hurricane season of 2004, the EAO assisted in the planning of an emergency update to NEMIS. Due to the amount of assistance requests, the System Development and Engineering Branch of ITSD developed an on-line capability to facilitate the individual assistance function of NEMIS. In doing so, the FEMA EA was used to assess the possible impacts to other applications and to ensure compliance with DHS standards.

Now on Pages 19 and 20

On pages 23 and 24 of the report, it states:

> "In 2001, FEMA developed an enterprise architecture document to serve as a guide to creating and implementing e-government initiatives. This road map has served FEMA well, documenting both major successes and key initiatives. For example, a few such initiatives were identified in the 2001 enterprise architecture and are still operational today… FEMA published its architecture in 2001, but has not fully updated it to reflect its integration into DHS. FEMA is working to transition this paper-based document to an electronic format so that it can be easily shared among DHS officials via the intranet. Currently, the "as-is" enterprise architecture is approximately 85 percent complete. FEMA has not yet begun work on the "to be" portion of the architecture, but expects to complete it by October 2005. Without a defined "to be" environment, FEMA is unable to provide a comprehensive road map for its proposed IT initiatives. These initiatives include NEMIS web enablement, which involves consolidation of some of the geographically-dispersed servers, as well as a number of IFMIS improvements as defined in the system's 2006 business case…Additionally, without a complete, communicated, "to be" road map, FEMA may not be able to address how its initiatives support or integrate with DHS-wide initiatives. As FEMA works to update its enterprise architecture, it must also consider department-wide initiatives which may impact on its key response and recovery processes and systems."

FEMA's response, while it is true it produced a paper version of the EA in May of 2001, it is NOT true that FEMA is currently using that version. In 2003, FEMA's CIO established an Enterprise Architecture Office (EAO) and hired a Chief Enterprise Architect in 2004. As a result, the FEMA EA Program has excelled tremendously. In fact, DHS has expressed an interest to use the FEMA EA as a spring broad for the Department. The FEMA EA was self assessed at a Level 3, in accordance with the OMB assessment criteria, in December 2004 and is on track to be assessed as a Level 4 this year.

The FEMA EAO has successfully developed the FEMA AS-IS Architecture and is currently making tremendous progress in developing the TO-Be Architecture in

accordance with the DHS Enterprise Architecture. In May and June of 2004, the FEMA EA was aligned to the DHS EA. Submittals of business, data, application and technical information were submitted and incorporated into the Homeland Security EA Version 2, dated June 24, 2004. In addition, to ensure alignment, FEMA Chief Enterprise Architect is a member of the DHS EA Center of Excellence (EACOE). The EACOE ensures that all DHS component EA programs are aligned with the DHS EA.

The EAO has successfully purchased and populated the Popkin, System Architect Modeling Application with FEMA AS-IS Architecture data. The application provides the EAO with the ability to conduct "what if" scenarios, to perform analysis on data and to assist managers in the decision making process. The FEMA EAO has also developed a five year EA Program Management Plan which defines the activities, timeline and resources needed over the next five years. The DHS Human Capital Center of Excellence cited this Program Management Plan as a potential model for DHS components.

Now on Page 34

On Page 38, under "Recommendation" it states: "Direct the EP&R CIO to complete the FEMA enterprise architecture, linked to the department wide architecture and ongoing initiatives that may impact EP&R operations." This recommendation is really not appropriate – the EA is never "complete," the EA process continues to evolve and mature as more applications, technologies, business processes, and requirements are generated for use and deployment. The FEMA EA is far ahead of most agencies. While it is true that the EA Program must continue to be developed and mature; as is the case for 100% of the EAs in the Federal government, we have aligned the FEMA EA with the DHS EA and have mapped our applications to DHS conceptual projects.

The FEMA CIO has made EA one of his top priorities and is dedicated and committed to its success.

We strongly believe there has been a great disconnect between the auditor and the EAO. The Enterprise Architect would welcome the opportunity to discuss the actions of the EAO and the EA accomplishments achieved.

FEMA's EA has been aligned to the Agency's program activity structure in FYHSP and the PPBE process. This program activity structure was created to directly support the execution of the DHS strategic objectives and metrics. This means that, through the EA, the Agency's IT activities are directly in line with the DHS strategic plan.

Now on Page 5

On page 8 the report states "In FY 2004, the EP&R directorate's CIO had a budget of approximately $80 million and a total of about 400 full-time and temporary employees to provide IT development and operational support for FEMA's response and recovery mission." We would like to point out that the resources cited are not exclusively dedicated to developing and operating IT for Response and Recovery.

8

Now on Page 5

On page 8 the third bullet should be changed to read "Logistics Information Management System-III (LIMS-III) provides personal property accountability as required by Public Law.

Now on Page 6

On page 9 of the report the OIG describes concerns that were found during prior assessments. The OIG does not include any information on the status of these items, giving the impression that the concerns have not been addressed. We believe this tends to provide an inaccurate and unfair picture of the status of IT in incident response and recovery.

Now on Page 6

On page 9 there is a statement regarding the "accuracy of data recorded in the LIMS system." We would like to address this issue by explaining that LIMS-III stores a continuous log of all transactions that are made in the system. With this log, specific transactions can be found and researched to determine the audit trail related to any transactions. While the audit can be done and has been utilized to search out a number of "data integrity" related issues. However, the process is arduous. The audit determined that when the data was converted from LIMS-II to LIMS-III some "dirty data" was brought along. Unfortunately, this data has caused some issues to arise from time to time which have been separately analyzed and corrected as appropriate. We believe LIMS data is becoming better and better in this regard. We have implemented a number of business rules related to this data that will help to correct the data as pertinent records are individually accessed. We know there are still a few "LIMS-II transfer" related issues to resolve and are gradually working to alleviate them.

Now on Page 10

On page 14 the report states "… the system does not have a "stopwatch" functionality to measure the elapsed time between contacting personnel of their need to deploy and their ultimate arrival at a disaster scene." We would like to point out that the ADD system has a "check-in" process that has a date/time stamp. Reports can easily be generated to measure the deployment time.

Now on Pages 10 and 13

On page 14 the report states "Similarly, LIMS provides no tracking of all of essential commodities such as ice and water needed by disaster victims." **On page 17** the report states "LIMS, FEMA's current logistics system, does not provide the type of up-to-date resource management that the National Incident Management System requires. Resource tracking and management was the source of numerous problems during the Florida hurricanes …." We would like to mention that LIMS was designed and built to track accountable property only. It has not been a requirement for logistics personnel to utilize LIMS-III to track bulk items or non-bar-coded items. It is a requirement for all accountable items to be entered into LIMS-III. Recently (when the National Disaster Medical System was transferred to FEMA), the capability to support bulk items was added into LIMS-III. A number of useful features were added and support for kitting was significantly enhanced. As a result, some warehouse managers utilize LIMS-III for their bulk items while others prefer to utilize their Excel spreadsheets to track the bulk items. LIMS-III would provide real-time visibility of inventory levels if all Logistical Center Managers and Accountable Property Officers utilized the system to track these items. It

would require that some means of providing power and connectivity at disaster sites forward of the Logistical Centers be provided to fully meet the desired definition of "real-time". LIMS-III was recently updated to 3-Tier Architecture and response times from the database to the web client are extremely fast.

During the support of 4 hurricanes in 2004, LIMS-III was 100% available. In response to issues which surfaced in the hurricanes of 2004, EP&R initiated the development of a Limited Deployment Option of a Total Asset Visibility System in Regions IV and VI. The Limited Deployment option is still in process. However, in Hurricanes Dennis and Emily, a part of that system, including satellite tracking devices, was used to track water shipments from the EP&R Palmetto Facility in Georgia to Mobilization Centers and Staging Areas in Florida, Alabama and Texas. Although not launched in its full operational mode, the system provided very valuable information on the timing of shipments, allowing realistic predictions of deliveries, an improved prediction of staffing needs at receiving locations, and interventions to reroute a couple of trucks following incorrect directions. The system was also used to track other EP&R assets, such as generators.

Now on Page 11

On page 15 the report describes recovery metrics and states "However, such goals are futile without effective means to accomplish them." NEMIS was developed by IT and includes the design for the development of a data warehouse and report generation capability that assimilates information from the National Finance Center, ADD, NEMIS, and IFMIS that should be used to measure performance. Considerable progress has been made recently to establish a comprehensive centralized reporting capability. The FEMA CIO agrees that performance metrics need to be adopted to measure achievement of disaster response goals. The CIO agrees that there is a need to define the requirements for capturing the appropriate response and recovery metrics, provide the resources to implement the information capture, and ensure that the mission goals and objectives are met. Program Offices need to identify the metrics so that our IT systems can capture the data for the Program Offices to measure effectiveness. (The CIO would like to point out that IFMIS, LIMS, and other systems were not developed or designed by IT, however, IT partners with the Business Units to provide support for these systems.)

Now on Page 14

On page 18 the report states "As FEMA moves forward with improving existing systems and pursuing new systems development, the EP&R CIO must ensure that the effects of DHS-wide initiatives, such as eMerge[2] and MAX HR, are considered and effectively support disaster response and recovery goals." EP&R is aware of these DHS-wide initiatives. Both the FEMA Human Resources Division (HRD) and the Information Technology Services Division (ITSD) are working collaboratively with the DHS Chief Human Capital Office (CHCO), the DHS IT Human Capital Center of Excellence, and other human resources (HR) representatives from other DHS components, in selecting the IT systems that will support MAX HR. The DHS/CHCO also works closely with each component's Senior Infrastructure Officer to coordinate Infrastructure, Desktop, and Help Desk requirements for all MAX HR systems. This leads to coordinated efforts between CHCO, HR representatives from the components, and Information and Application Delivery to identify obstacles and solutions to achieve successful

implementations of these and existing legacy systems. The HRD and the ITSD will continue to work in conjunction with DHS as MAX HR is rolled-out to ensure that FEMA continues to successfully carry out its response and recovery mission. FEMA's Property Management Unit (PMU) participated in the DHS Logistics Steering Committee and has chaired the committee to advance the logistics system definition, in support of the eMerge^2 initiative.

Now on Page 14

On page 18 the report states "the EP&R CIO's office provided significant customer support to IT users assisting disaster response and recovery efforts related to the 2004 Florida hurricanes. However, overall systems guidance and training could be improved. Specifically, EP&R has reasonably up-to-date online systems manuals, but these manuals are not adequate to support business processes … although EP&R training is good, funding restrictions limit the number of personnel who receive the training." EP&R recognizes the need to ensure that system users have the knowledge and information necessary to perform their jobs. Soon we expect that the IT staff in the regions will report to the CIO. That change will help the CIO in defining training requirements and working with the Business Units and the training staff at Emmitsburg, Maryland to integrate training materials and improve training methods. Actions will also be taken to ensure awareness of the training materials that are available.

Now on Page 19

On page 22 the report states "The EP&R systems environment, however, is not integrated and does not support effective information exchange. Consequently, during disasters, the systems are not able to handle increased workloads effectively, are not adaptable to change, and lack needed capabilities." ITSD believes that systems integration for EP&R mission execution is absolutely essential and should proceed while integrating DHS corporate programs such as eMerge^2, and MAX HR into the mission application solutions.

Now on Page 20

On page 24 the discussion under the second paragraph under the heading "Databases Are Not Fully Integrated, " should be omitted because it is not relevant to either database integration or mission application integration. The CIO would like to advise that when NEMIS was developed, FEMA created a state-of-the-art distributed client-server architecture, providing each region with its own set of servers to support regional operations with limited impact on the FEMA telecommunications network and its bandwidth limitations.

Now on Pages 21 and 22

On page 25 the report states "FEMA systems do not support effective or efficient coordination of deployment operations because there is no sharing of information." **On page 26** the report states "Further, the lack of integration between ADD and LIMS hinders FEMA from providing the appropriate number and combination of people and supplies to meet the level of need at disaster locations." The CIO is pleased to note that the report acknowledges that IT officials agree that it is essential to integrate systems to better support mission requirements, but that this decision must be made in collaboration with the system owners and program officials, and also consider DHS-wide direction and programs. In the DHS' eMerge^2 solution the "Logistics Management" solution was

specifically excluded. This was due to the complex differences between Logistic System requirements of the various components within DHS. At present DHS continues to review direction and alternatives for the future. The pre-staging and kitting capabilities of LIMS-III have been substantially improved, both operationally as well as through Standard Operating Procedures, in the last year. This speeds up substantially the speed of dispatching kits and pre-staged supplies.

Now on Page 22

The discussion **on page 26** with the example cited is partially incorrect. There were 600 to 800 tractor-trailers arriving at one staging area within a 24-to-36-hour period, not all of the tractor-trailers came from FEMA Logistics Centers which LIMS-III manages. Most of the tractor-trailers transported water, ice and/or tarps coming directly from suppliers to the staging area as directed by other Federal Agencies.

Now on Page 22

On page 26 the report states "…EP&R response and recovery systems do not share information with those used by major stakeholders in state governments….Currently, state users can access NEMIS, but not directly from their desktops." Cyber security requirements prevent the States from directly accessing NEMIS from their desktops.

Now on Page 23

We disagree with the statement **on page 27** that our systems were unable to handle increased workloads required to support disaster application processing during the 2004 hurricanes. FEMA's major systems can handle increased workloads but not 300 times the normal designed workload, as was the case during the 2004 hurricane season, the period addressed in this report. IT and Recovery staff worked heroically during that period to keep the system going and succeeded in successfully registering and assisting an unprecedented number of disaster victims. EP&R expects to be continually challenged in keeping its IT systems and processes current since change is a constant in emergency management operations. The CIO acknowledges the shortfalls in our current systems. While improvements are continually being made to our IT systems and solutions in response to pressing operational needs of our business units, the CIO recognizes the value of taking the time needed to define and document systems requirements fully and evaluate viable alternatives. Unfortunately, meeting day-to-day operational requirements and the lack of resources have not allowed FEMA the luxury of doing extensive requirements capture and development prior to making needed system upgrades in the past several years.

Now on Page 26

On page 30 the report states "Response and recovery program personnel said that FEMA systems did not provide useful reports regarding ongoing operations." LIMS-III has substantial reporting capabilities for both automatic and manual reports with minimal efforts. These custom reports, once created, can be dumped into specific network directories or emailed to requesting users. In the manual report category, LIMS-III has an ad-hoc reporting capability that is flexible, easy to use and useful. In addition, NEMIS has numerous reports available to operational personnel which are used daily during a response/recovery action.

12

Now on Pages 26-29 and 10

Regarding the issues presented in the report **on pages 30-32** regarding real-time resource tracking issues, EP&R is currently developing a tracking capability under the Total Asset Visibility project mentioned on page 9.

Now on Pages 29-32

In response to the information presented **on pages 33-36** regarding the updating of NEMIS requirements and the need for an alternatives analysis, the report correctly notes the responsibility of management at all levels to recognize and act on these problems. The CIO intends to elicit broad stakeholder participation in the requirements definition process for the e-NEMIS initiative. The CIO understands the need to integrate systems and is ensuring that new initiatives conform to the FEMA and DHS EA. Upgrading IFMIS is also a necessity due to the current status of the eMerge^2 initiative. FEMA's deployment system is another area that requires significant investment to upgrade.

Now on Page 32

On page 36 the report states that "… nine months prior to the 2004 hurricanes, the EP&R CIO office convinced reluctant program offices to fund development of an online registration capability for NEMIS." The Recovery Division fully supported the initiative from the outset and assisted in the development. The CIO's office made a tremendous effort to stand up the online registration in record time and this was an exemplary achievement since it provides another avenue for disaster victims to register for assistance. It was achieved in time to make a difference in the response to the 2004 hurricanes. IT did an outstanding job in supporting the hurricane recovery operations and deserves great credit for keeping the system functioning under the most trying conditions. The NEMIS system reduced the time to deliver assistance from weeks to days. Representatives from the Recovery Division have stated it is important to appreciate how much IT has allowed them to do and how great the potential is to do much more.

Information Management Division

Sondra McCauley, Director
Richard Harsche, Audit Manager
Meghan Sanborn, Auditor
Steven Staats, Auditor

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
EP&R Under Secretary
General Counsel
Executive Secretariat
DHS CIO
EP&R CIO
DHS Office of Security
DHS Audit Liaison
EP&R Audit Liaison
DHS Public Affairs
DHS Legislative Affairs
FEMA Public Affairs
FEMA Congressional Affairs

Office of Management and Budget

Homeland Bureau Chief
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.