United States Government Accountability Office

Report to Congressional Requesters

April 2016

INFORMATION TECHNOLOGY

FEMA Needs to Address Management Weaknesses to Improve Its Systems

Accessible Version

GAO-16-306

April 2016

INFORMATION TECHNOLOGY

FEMA Needs to Address Management Weaknesses to Improve Its Systems

GAO Highlights

Highlights of GAO-16-306, a report to congressional requesters

Why GAO Did This Study

FEMA, a component agency of the Department of Homeland Security (DHS), leads federal efforts to mitigate, respond to, and recover from disasters. In the wake of Hurricane Katrina, the largest natural disaster in U.S. history, Congress passed the Post-Katrina Emergency Management Reform Act of 2006. This act required FEMA to address shortcomings identified in the preparation for and response to Katrina, including improving the agency's IT programs, which are critical to its ability to respond to natural disasters and other emergencies.

GAO was asked to review FEMA's IT system improvement efforts. This report (1) identifies challenges to ensuring the agency's IT systems adequately support its disaster response efforts and (2) assesses the extent to which FEMA has implemented key IT management controls for selected emergency management programs. GAO analyzed FEMA documentation (e.g., FEMA's Hurricane Sandy After-Action Report), interviewed officials, and assessed its implementation of IT management best practices for three selected programs.

What GAO Recommends

GAO recommends that FEMA fully define its investment board's roles and responsibilities and procedures for selecting and overseeing investments, update its strategic plan and complete plans for IT modernization, and establish time frames for completing workforce planning efforts. FEMA should also establish policies and guidance for implementing key IT management controls. DHS concurred with the recommendations.

View GAO-16-306. For more information, contact Carol R. Cha at (202) 512-4456 or ChaC@gao.gov.

What GAO Found

The Federal Emergency Management Agency (FEMA) faces the following challenges in ensuring that its information technology (IT) programs adequately support the agency's ability to respond to major disasters:

- **Governance and oversight:** FEMA established an investment review board to select and oversee IT investments, as called for by leading practices. But the board has not fully defined roles and responsibilities of key members, working groups, and individuals, and it does not have clearly defined procedures for selecting and overseeing investments. As a result, the agency lacks adequate visibility into and oversight of IT investment decisions and activities.
- **IT modernization:** FEMA has begun to take steps to modernize its IT environment, but key planning documents are not current and complete. For example, the agency has an IT strategic plan and is currently drafting its modernization plan; however, the plans do not reflect the agency's current goals and objectives. Further, the IT strategic plan describes the Chief Information Officer's (CIO) mission, goals, and objectives through fiscal year 2016, but has not been updated since 2013. In addition, while the Office of the CIO is currently drafting the agency's IT modernization plan, including an implementation strategy and an overall schedule, it is not yet final. As a result, the agency is limited in its ability to move toward its goal to modernize its systems and eliminate duplicative IT investments.
- **Workforce planning:** The agency has not yet established time frames to address long-standing workforce management challenges. For example, while it conducted a workforce assessment to identify skill levels of employees in the agency's Office of the CIO, it has not completed recommended actions called for by this assessment. In addition, its workforce planning efforts have not included an assessment of the many IT staff located in the agency's regions and other offices. Consequently, FEMA has less assurance that its IT workforce will have the skills needed to successfully manage its programs.

None of the three emergency management programs GAO selected for this review had fully implemented key IT management controls in the areas of risk management, requirements development, project planning, and systems testing and integration. Specifically, the three selected emergency management programs inconsistently implemented these practices by, for example, not always developing adequate risk mitigation plans, establishing processes for requirements management, developing and updating schedules and cost estimates, and ensuring complete and adequate system testing along with systems integration plans. These weaknesses were due, in part, to a lack of FEMA policies to guide programs in implementing these key IT management controls. Until FEMA fully establishes and implements such policies and controls, it has limited assurance that these programs will cost-effectively support its disaster response efforts.

Contents

Abbreviations

CIO	Chief Information Officer
CMMI-ACQ	Capability Maturity Model® Integration for Acquisition
DAIP	Disaster Assistance Improvement Program
DHS	Department of Homeland Security
EADIS	Enterprise Applications Development, Integration, and Sustainment
EMMIE	Emergency Management Mission Integrated Environment
FEMA	Federal Emergency Management Agency
IEEE	Institute of Electrical and Electronics Engineers
IG	inspector general
IPAWS	Integrated Public Alert and Warning System
IT	information technology
OCIO	Office of the Chief Information Officer
PMBOK® Guide	Project Management Institute's Guide to the Project Management Body of Knowledge
Post-Katrina Act	Post-Katrina Emergency Management Reform Act of 2006
SEI	Software Engineering Institute

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

April 5, 2016

Congressional Requesters

The Federal Emergency Management Agency (FEMA), a component of the Department of Homeland Security (DHS), leads the federal effort to mitigate, respond to, and recover from disasters. FEMA is responsible for saving lives and protecting property and public health and safety in a natural disaster, act of terrorism, or other manmade disaster. To meet its mission, it relies heavily on the use of information technology (IT). According to FEMA's IT investment portfolio for fiscal year 2015, the agency reportedly spent at least $366.4 million for its IT investments.

Hurricane Katrina in 2005 was the largest, most destructive natural disaster in our nation's history. FEMA estimated that Hurricane Katrina caused an estimated $108 billion in damages. Following the federal response to Hurricane Katrina in 2005, the Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act) was enacted into law.[1] The act enhanced FEMA responsibilities to lead the country's emergency management system. In doing so, the act required FEMA to address the shortcomings identified in the preparation for and response to Hurricane Katrina. For example, it required the FEMA Administrator, in coordination with the DHS Chief Information Officer (CIO), to take appropriate measures to update and improve the agency's IT systems.

In view of the act's requirements, you asked us to review FEMA's efforts to improve its IT systems. Our objectives were to (1) identify challenges associated with ensuring FEMA's IT systems adequately support the agency's ability to respond to major disasters and (2) assess the extent to which FEMA has implemented key IT management controls for selected emergency management systems.

To address the first objective, we obtained and analyzed FEMA documentation (e.g., IT strategic plans, FEMA's Hurricane Sandy After-Action Report), prior GAO reports, and DHS inspector general (IG)

[1]The Post-Katrina Act was enacted as Title VI of the Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109-295, 120 Stat. 1355, 1394-1463 (2006).

reports to identify challenges associated with ensuring FEMA's IT systems adequately support its ability to respond to major disasters. We also interviewed officials from the National Advisory Council; the Disaster Emergency Communications Division; Regions 2, 4, and 6; Mobile Emergency Response Center (Thomasville, Georgia); and the National Processing Center (Maryland). Further, we interviewed agency officials from FEMA's Office of the Chief Information Officer (OCIO), its Office of Policy & Program Analysis, and DHS's IG office to obtain their perspectives on the challenges associated with FEMA's IT systems. We then aggregated the key challenges. To determine the extent to which FEMA had adequate controls in place to address these challenges, we compared the agency's efforts to best practices we have identified in the areas of IT investment management,[2] human capital management,[3] and strategic planning.[4]

For the second objective, we selected three FEMA IT programs to determine the extent to which FEMA has implemented key management controls. The three programs we reviewed were the Disaster Assistance Improvement Program (DAIP), Emergency Management Mission Integrated Environment (EMMIE), and the Integrated Public Alert and Warning System (IPAWS). In selecting these programs, we relied on the Office of Management and Budget's exhibit 53 and applied selection criteria, including whether the program was associated with objectives of the systems identified in the Post-Katrina Act or had spending in fiscal year 2015. We then identified key practices in the areas of risk management, requirements management, project planning, and systems integration and testing from the Software Engineering Institute's Capability Maturity Model® Integration for Acquisition (CMMI-ACQ) and the Project Management Institute's Guide to the Project Management

[2]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (Supersedes AIMD-10.1.23),* GAO-04-394G (Washington, D.C.: March 2004).

[3]GAO, *A Model of Strategic Human Capital Management,* GAO-02-373SP (Washington, D.C.: March 2002); *Human Capital: Key Principles for Effective Strategic Workforce Planning,* GAO-04-39 (Washington, D.C.: Dec. 11, 2003); and *Information Technology: FDA Needs to Establish Key Plans and Processes for Guiding Systems Modernization Efforts,* GAO-09-523 (Washington, D.C.: June 2, 2009).

[4]GAO, *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization*, GAO-12-495 (Washington, D.C.: Apr. 26, 2012).

Body of Knowledge (PMBOK® Guide).[5] To determine the extent to which each of the three programs had implemented key practices in these areas, we assessed each of the three program's relevant documentation against these criteria.

We conducted this performance audit from January 2015 to April 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Additional details of our scope and methodology are contained in appendix I.

Background

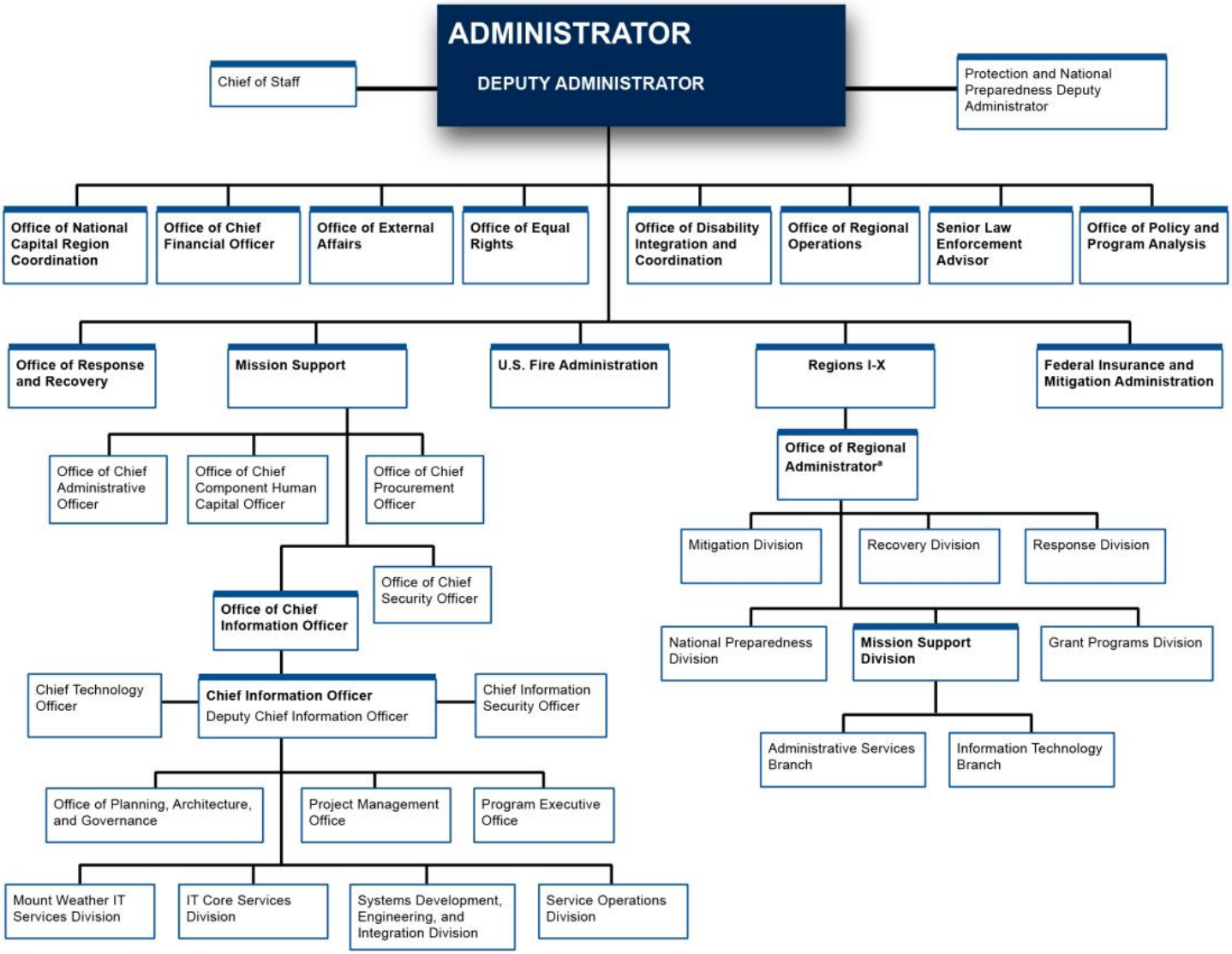
FEMA's mission is to support citizens and first responders to build, sustain, and improve the nation's capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. It supplies immediate needs, such as ice, water, food, and temporary housing in response to disasters. 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.

To support its mission, FEMA has more than 4,900 full-time employees located at its headquarters in Washington, D.C., its 10 regional offices, two area offices, five recovery offices, and various sites across the country. Additionally, FEMA has more than 3,700 standby disaster assistance employees who are available for disaster deployment and nearly 5,000 reserve employees. The agency also partners with other organizations that are part of the nation's emergency management system, including 27 federal agencies, state and local emergency management agencies, and the American Red Cross. For fiscal year 2015, FEMA's budget request was approximately $14.7 billion, representing 24 percent of the DHS budget request of approximately $60.9 billion.

[5]Software Engineering Institute, *Capability Maturity Model® Integration for Acquisition* (CMMI-ACQ), Version 1.3 (Pittsburgh, Pa.: November 2010); Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Fifth Edition,* (Newton Square, Pa.: 2013).

The agency is headed by an Administrator and its primary mission areas include Federal Insurance and Mitigation, Mission Support, Protection and National Preparedness, Regional Operations, Response and Recovery, and United States Fire Administration, as depicted in figure 1. Each component has multiple directorates and program offices that carry out disaster response missions and functions, as well as administrative support.

Figure 1: FEMA's Streamlined Organization Structure, as of October 2015



Source: GAO analysis of U.S. Federal Emergency Management Agency data. | GAO-16-306

[a]The Office of the Regional Administration structure is an example of one of the regions.

Within the Mission Support component, the OCIO is responsible for developing, enhancing and maintaining the IT systems, and increasing efficiencies and cooperation across the entire FEMA organization. OCIO partners with FEMA programs and regional offices to provide for systems development, testing, implementation, and operations and maintenance

efforts. For example, the regions have IT employees that report directly to the regional leadership; these staff are to coordinate with the OCIO on IT responsibilities such as managing and supporting IT hardware and software (e.g., needs assessment and hardware issuance, inventory, and decommissioning).

According to OCIO officials, in fiscal year 2015, FEMA's OCIO was made up of nearly 300 federal employees and 228 contractors and had a budget of approximately $122.1 million, which is about one-third of the FEMA IT budget for fiscal year 2015. As shown in figure 1, the office is organized into nine offices and divisions to plan and manage FEMA's IT environment.

FEMA's IT Environment

IT systems play a critical role in supporting FEMA's response and recovery efforts. For example:

- The Disaster Assistance Improvement Program (DAIP) has a major interagency support system that provides disaster survivors an online registration vehicle (including mobile capabilities) to apply for disaster assistance from 17 federal partners, including Individual Assistance from FEMA, and is managed by FEMA's Office of Response and Recovery. DAIP is currently in the mixed life cycle phase of the systems engineering life cycle; spending on the program was about $13.7 million in fiscal year 2015, of which $12.9 million is from FEMA and the rest is from other federal partners.

- The Emergency Management Mission Integrated Environment (EMMIE) program has an Internet-based enterprise-wide electronic system for FEMA to manage grants throughout the entire grant life cycle using a standardized web-based interface, and is also managed by FEMA's Office of Response and Recovery. EMMIE is currently in the operations and maintenance phase of the systems engineering life cycle; the agency spent about $2.7 million on the program in fiscal year 2015. FEMA does not plan to make any enhancements to EMMIE's functionality because the system is scheduled to be decommissioned once the agency's Grants Management Modernization system, the enterprise-wide capability for the management of all FEMA disaster and non-disaster grants, is implemented. According to the EMMIE officials, the implementation date is estimated to occur in 2020.

- The Integrated Public Alert and Warning System (IPAWS) program has a major system that provides a broad range of messaging capabilities through multiple pathways to ensure that the delivery of alerts and warnings reaches more people, and is managed by FEMA's National Continuity Programs Directorate. IPAWS is currently in the mixed life cycle phase of the systems engineering life cycle; FEMA spent about $10.9 million on the program in fiscal year 2015.

In addition, FEMA's Enterprise Applications Development, Integration, and Sustainment (EADIS) program is intended to develop and integrate new and modernized applications while supporting the sustainment of existing technology, services, and applications. There are almost 80 FEMA systems, including grant tracking, family locator, and assessment reporting, that are supported by EADIS. The current FEMA EADIS contract consists of many individual platform-specific work orders that encompass a spectrum of new and old technologies, architectures, platforms, and tools that include a variety of personal computer-based, client-server, web-based, and service-oriented components.[6]

OCIO is also responsible for managing and maintaining the networks, databases, desktops, and telephone systems to support the operations of permanent facilities at FEMA. The CIO is also 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 is to assist internal 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.

[6]In 2008, FEMA issued a $1 billion task order for EADIS to IBM to serve as a single developer and applications integrator for all applications developed in pursuit of FEMA's missions. In December 2014, FEMA extended the task order 1 year to provide IBM more time to develop a comprehensive contract solution to support dozens of disaster recovery and legacy IT systems across FEMA. EADIS is a cost-plus-award-fee task order issued by FEMA under the DHS Enterprise Acquisition Gateway for Leading-Edge Solutions for all agency applications development.

GAO and Inspector General Reviews Have Recommended Improvements to FEMA's IT Management

Prior GAO and IG assessments have identified concerns with several aspects of FEMA's IT management.[7] For example:

- In 2012, we reported that a subsidiary project for FEMA's DAIP, which included usability enhancements to the agency's DisasterAssistance.gov website, was delayed.[8] Specifically, technical issues in establishing a testing and development environment that matched the production environment delayed project testing and caused cost and schedule shortfalls. For example, costs for a project under FEMA's DAIP investment rose approximately 27 percent ($210,000) due, in part, to the delayed deployment of another investment. We recommended that the department define and document corrective actions for these shortfalls. The department agreed with our recommendation and subsequently developed a remediation plan for most of the shortfalls to limit the negative impact.

- In 2011, we reported that FEMA faced significant management challenges in areas that affect the National Flood Insurance Program, which is to provide direct disaster relief after floods.[9] These challenges included ineffective collaboration among offices within the agency that were responsible for administering the program, including the Mission Support office, which provided mission-critical functions, such as IT, acquisition, and financial management. To address these challenges, we recommended, among other things, that FEMA develop protocols to encourage and monitor collaboration between the office that administers the National Flood Insurance Program and relevant support offices, including those for IT, acquisition management, and financial management. In response, the Mission Support Bureau had an ongoing effort to meet with FEMA program

[7]GAO, *Emergency Preparedness: Improved Planning and Coordination Necessary for Modernization and Integration of Public Alert and Warning System*, GAO-09-834 (Washington, D.C.: Sept. 9, 2009); *Disaster Assistance Workforce: FEMA Could Enhance Human Capital Management and Training,* GAO-12-538 (Washington, D.C.: May, 25, 2012); *Emergency Alerting: Capabilities Have Improved, but Additional Guidance and Testing Are Needed*, GAO-13-375 (Washington, D.C.: Apr. 24, 2013); and *Federal Emergency Management Agency: Additional Planning and Data Collection Could Help Improve Workforce Management Efforts,* GAO-15-437 (Washington, D.C.: July 9, 2015).

[8]GAO, *Information Technology: DHS Needs to Enhance Management of Cost and Schedule for Major Investments*, GAO-12-904 (Washington, D.C.: Sept. 26, 2012).

[9]GAO, *FEMA: Action Needed to Improve Administration of the National Flood Insurance Program,* GAO-11-297 (Washington, D.C.: June 9, 2011).

offices to better understand the needs of their customers and encourage collaboration between the Bureau and these offices. In 2015, we identified this program on our high-risk list due to the structural weaknesses on how the program is funded and weaknesses in management and program operations.[10] In response, officials stated that the agency is in the acquisition stage for a new IT system for the entire National Flood Insurance Program.

- We also reported, in 2009, that FEMA faced coordination issues and technical challenges in developing and implementing the IPAWS program.[11] Specifically, the agency faced challenges related to systems integration and development. Subsequently, we recommended that the Secretary of Homeland Security direct the Administrator of FEMA, as IPAWS is developed and deployed, to establish and implement a plan to verify, among other things, the dependability and effectiveness of systems used to disseminate alerts. DHS agreed with our recommendation and stated that FEMA was developing an IPAWS Strategic Plan and had modified existing plans to address these issues.

Similarly, in November 2015, the DHS IG reported that FEMA has taken steps to improve its IT management since the IG's 2011 audit, but more remained to be done.[12] Specifically, in 2011, the IG had reported that FEMA IT systems did not fully support mission needs, were not integrated, and did not fully provide needed capabilities because, in part, they had been developed, patched, and interconnected in an ad hoc manner.[13] As a result of system limitations, the IG noted that end users were engaged in inefficient, time-consuming business practices, creating their own tools such as spreadsheets and databases. Accordingly, the IG recommended that the CIO implement a plan of action and milestones to address the integration and reporting limitations of existing systems. The IG also recommended that the CIO implement and enforce a

[10]GAO, *High-Risk Series: An Update,* GAO-15-290 (Washington, D.C.: Feb 11, 2015).

[11]GAO-09-834.

[12]Department of Homeland Security Office of Inspector General, *FEMA Faces Challenges in Managing Information Technology,* OIG-16-10 (Washington, D.C.: November 20, 2015).

[13]Department of Homeland Security Office of Inspector General, *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology,* OIG-11-69 (Washington, D.C.: April 1, 2011).

standardized, agency-wide process that sufficiently defines and prioritizes the acquisition, development, operation, and maintenance requirements for all systems. In November 2015, the IG reported that this recommendation remained open.

FEMA Faces IT Management and Workforce Challenges

FEMA faces a number of challenges in ensuring that its IT systems adequately support the agency's ability to respond to major disasters. Specifically, the agency has not (1) established a sufficient framework for providing governance and oversight of its IT investments, (2) developed adequate plans for modernizing its IT environment to reduce its reliance on duplicative and outdated systems, and (3) taken sufficient steps to address gaps in its IT workforce. These weaknesses can be attributed, in part, to the agency not viewing these challenges as a management priority. Until it adequately addresses these challenges, FEMA will be hindered in ensuring that its IT systems provide the needed support for its disaster response mission.

FEMA's Approach to IT Governance Does Not Adequately Address Key Elements

GAO's IT investment management framework is composed of five progressive stages of maturity that mark an agency's level of sophistication with regard to its IT investment management capabilities.[14] Such capabilities are essential to the governance of an organization's IT investments. At the Stage 2 level of maturity, an organization lays the foundation for sound IT investment processes that help it attain successful, predictable, and repeatable investment control processes at the project level. These processes focus on the agency's ability to select, oversee, and review IT projects.

According to the framework, a foundational component of effective IT investment management includes the following practices:

- Establishing an IT investment review board composed of senior executives from both IT and business units that is responsible for defining and implementing the department's IT investment governance process. In instituting an investment board, the organization's IT investment process guidance should lay out the

[14] GAO-04-394G.

roles of key boards, working groups, and individuals involved in the organization's IT investment processes.

- Establishing and implementing policies and procedures for selecting and reselecting IT investments that meet the agency's needs, and integrate these with funding and selection decisions. This includes selecting projects by identifying and analyzing projects' risks and returns before committing any significant funds to them and selecting those that will best support the agency's mission needs.

- Establishing and implementing policies and procedures for overseeing IT projects by reviewing the progress of projects against expectations and taking corrective action when these expectations are not being met.

While FEMA has begun to address these practices, its investment governance framework does not adequately incorporate key elements:

- Establishing IT governance boards. In September 2014, the agency reestablished its IT Governance Board, co-chaired by the Deputy Administrator and the Chief Information Officer and made up of senior leadership from each of FEMA's major headquarters program and support organizations and three Regional Administrators. Subsequently, in May 2015, a charter was finalized that documented the mission of the board to assist and support leaders in their responsibility to ensure that IT roles, responsibilities, and resources are properly aligned with business needs; IT performance is managed; risks are mitigated; and benefits are realized.

Since the board was reestablished, it has met on a monthly basis to review progress and issues related to FEMA's IT. For example, in July 2015, the board discussed the need for a detailed breakdown of the tasks associated with the $68.7 million EADIS task order. In particular, the board members stated that some of the lack of detail could be attributed to funds being obligated to the contractor without having firm requirements. During the September 2015 governance meeting, the OCIO discussed, among other things, their approach for strengthening service-level management capabilities by conducting a series of workshops with FEMA leadership and programs.

- While the IT Governance Board is operating and has defined the membership of the board, it has not defined the roles and responsibilities of key board members, working groups, and individuals involved in the organization's IT investment processes. For

example, the agency's charter describes the role of the board's co-chairs and Chief of Staff, but it does not specify the responsibilities of the other board members, including the Regional Administrators.

- In addition, FEMA has not defined how its regional working group is to collaborate with the IT Governance Board. In April 2014, FEMA established the Regional IT Chief Committee, a subordinate committee to the OCIO, co-chaired by the IT Disaster Operations Branch Chief and an elected individual from the group. According to the draft charter, this committee is intended to be responsible for providing information to the governance board to ensure that IT initiatives will be viewed from a field perspective during all phases. Specifically, this committee is to serve as the IT authority on regional resources and capabilities, including developing and maintaining inventories of regional IT assets and working with senior IT management to apply standardization across FEMA regions.

- However, the charter does not define the procedures for how the committee is to collaborate with the IT Governance Board to carry out its duties. In particular, according to FEMA OCIO officials, Regional Administrators regularly update each other on significant topics and issues, but this is done on an ad hoc basis. Further, the committee's charter is not yet finalized and, according to FEMA officials, the current membership is being reviewed to include the CIO and Deputy CIO. Nonetheless, the officials did not identify time frames for finalizing the charter. Without clearly defined roles and responsibilities, FEMA has less assurance that investments will be reviewed by those with the appropriate authority and aligned with agency goals.

- Establishing policies and procedures for selecting investments that meet business needs. While FEMA's governance board has policies for selecting and reselecting investments, it lacks procedures for doing so. Specifically, while the charter calls for the review and selection of IT investments at least annually by recommending and presenting a list of IT investments proposed for funding to the board and executive-level business decision making authority, it does not specify the procedures to do so. In addition, FEMA's charter states that the board is to make a recommendation to terminate or retire an investment from the portfolio to the IT investment business owner, but it does not specify the process for doing so. In the absence of such procedures, FEMA's decision makers lack a common understanding of the process and the cost, benefit, schedule, and risk criteria that will be used to select or reselect IT projects.

- Establishing policies and procedures for providing investment oversight. The agency's board does not have policy and procedures to ensure that corrective actions and related efforts are executed by the project management team and tracked by the board until the desired outcomes occur. In particular, FEMA requires the investment board to review and approve project planning materials, such as business cases, project plans, and acquisition strategies for addressing system issues. However, there are no procedural rules for the investment board's operation and for decision making during project oversight or that require corrective actions when the project deviates significantly from its plan. Consequently, FEMA cannot ensure that investments are meeting cost and schedule expectations and that appropriate actions are taken if these expectations are not being met.

FEMA's Key Plans to Modernize Aging Legacy Systems and Consolidate Duplicative Systems Are Not Current or Complete

Strategic planning is essential for an organization to define what it seeks to accomplish, identify strategies to efficiently achieve the desired results, and effectively guide modernization efforts. Key elements of IT strategic planning include an IT strategic plan with well-defined goals, strategies, measures, and timelines to guide these efforts. Our prior work has found that, according to best practices, an IT strategic plan should define the agency's vision and provide a road map to help align information resources with business strategies and investment decisions.[15] Additionally, our work has found that effective modernization planning includes defining the scope of the effort, an implementation strategy, and a schedule, as well as establishing results-oriented goals and measures.[16]

FEMA has strategic planning efforts under way to guide its IT modernization, but the plans are not current and not yet complete. For example, the IT strategic plan describes the CIO's mission, goals, and objectives for fiscal year 2013 through 2016, but has not been updated since 2013, even though the plan calls for an annual update. Furthermore, it contains elements that are no longer current with FEMA's ongoing modernization efforts, as the following examples illustrate:

[15]GAO-12-495.

[16]GAO, *Information Technology: HUD's Expenditure Plan Satisfied Statutory Conditions; Sustained Controls and Modernization Approach Needed,* GAO-14-283 (Washington, D.C.: Feb. 12, 2014).

- The plan is intended to align with the FEMA strategic plan, which has been updated since to reflect fiscal years 2014 to 2018 and the DHS IT strategic plan, which has been updated to reflect fiscal years 2015 to 2018.

- The plan identifies specific CIO priorities only for fiscal year 2012 to 2013.

OCIO officials acknowledged that the plan is no longer current. The CIO explained that updating the current strategic plan had not been a priority and the agency would rather spend resources on developing a new plan that incorporates a global FEMA IT strategic vision. However, a date by which a revised plan will be completed has not been established. Establishing a current strategic plan would allow the agency to align its information resources with its business strategies and investment decisions.

According to FEMA OCIO officials, modernizing FEMA's current IT environment is important because it suffers from duplication and inefficiencies. For example, according to OCIO officials, its systems are not intuitive and they require managers and leaders to spend significant time logging into various systems to complete and approve numerous forms. Regional staffs are frustrated by having to remember 18 to 20 passwords in order to access systems that minimally support their work needs. According to OCIO officials, the agency's systems need to be replaced with more secure and easy to use tools that better support activities focused on disaster survivors. The current systems used to deliver and manage these services have been neglected or cobbled together based on immediate needs ("disaster-driven"), often without an orchestrated FEMA-wide approach for acquiring and managing IT. Additionally, over half of the physical servers in FEMA are more than 5 years old, increasing the risk of hardware failures that could affect the delivery of mission-essential systems.

While the CIO has begun to develop a draft IT modernization plan that includes the scope of its efforts, an implementation strategy, and schedule of its overall modernization effort, it is not yet complete. Specifically, FEMA OCIO officials stated that the IT modernization plan is to provide the steps and investments needed to realize a transformed IT. According to the OCIO, the plan is to be completed by April 2016. Without complete and up-to-date planning documents, including the strategic and modernization plans, FEMA will be unable to move toward its ultimate goal of modernizing and eliminating duplicative IT investments.

FEMA Has Gaps in Its IT Workforce Planning Efforts

Key to an agency's success in managing its IT systems is sustaining a workforce with the necessary knowledge, skills, and abilities to execute a range of management functions that support the agency's mission and goals.[17] Achieving such a workforce depends on having effective human capital management, which includes assessing current and future agency skill needs by, for example, analyzing the gaps between current skills and future needs, and developing strategies for filling the gaps. Taking such steps is consistent with activities outlined in human capital management models that we and the Office of Personnel Management have developed.[18]

In July 2015, we reported that FEMA had not yet resolved and fully addressed various long-standing workforce management challenges in completing and integrating its strategic workforce planning efforts, which we have identified since 2007.[19] In particular, we reported that FEMA had taken or was planning various actions to address a number of these issues. However, since many of these efforts were ongoing and not yet completed, it was not clear whether they would be effective or to what extent they would address our prior recommendations and challenges that we and others had identified.

Similarly, while the agency has taken initial steps to assess the needs of its IT workforce, it has not yet established time frames for completing workforce planning efforts and it lacks an understanding of its regional IT workforce. In April 2014, OCIO conducted two activities to obtain a greater understanding of FEMA OCIO personnel resources. For example, it completed a Workforce Capability Survey designed to determine the skill levels of OCIO employees and a workload analysis in which almost 800 IT activities performed by the OCIO were assessed to determine staffing requirements. The report resulting from these activities noted that the FEMA OCIO organization had a shortage of 150 full-time equivalent positions.[20] Accordingly, the report recommended three actions for the

[17]GAO-02-373SP, GAO-04-39, and GAO-09-523.

[18]Office of Personnel Management, *Human Capital Assessment and Accountability Framework—Systems, Standards, and Metrics* (http://www.opm.gov/hcaaf_resource_center/).

[19]GAO-15-437.

[20]FEMA, *OCIO IT Workforce Requirements, Gaps, and Actions* (April 2014).

OCIO to close the workforce gaps, including to develop and implement (1) a human capital management strategy, (2) an OCIO workforce staffing plan based on in-depth staffing analysis and managed at the corporate governance level, and (3) an OCIO workforce training plan based on in-depth analysis and managed in conjunction with the staffing plan at the corporate governance level. However, these actions have not yet been completed. According to the CIO, the agency will revisit this report, including the recommendations, upon completion of its IT modernization plan.

Additionally, the analysis FEMA conducted only covered the OCIO, and according to agency officials, there are significant numbers of IT staff and related expenditures outside this office, including in the regions. The regions included in our review all stated that IT workforce planning was a significant challenge. For example, IT officials from one regional office stated that the biggest challenge it faces is a lack of IT staff (e.g., highly skilled computer engineers and network engineers). Further, officials from another regional office stated they do not have enough full-time equivalents to handle disasters. Thus, they need to utilize external resources, which take additional time to deploy. While the OCIO officials stated that the office is in the process of baselining the number of IT staff who perform IT functions in the regions and offices, it has not yet done so. According to the report and CIO, analyses of regions and offices will be integrated into future workforce planning efforts. Fully assessing and implementing actions to close these competency gaps will be critical to ensuring FEMA has the skills it needs to adequately support its ability to respond to major disasters.

Without a better understanding of its current IT workforce, including staff in all regions and offices, FEMA will be unable to solve its workforce planning needs, as the CIO has acknowledged. In addition, until it fully develops plans for modernizing its IT infrastructure (as previously discussed), the agency will not be positioned to assess the skills its workforce will need in the future.

The weaknesses in governance, IT strategic planning, and workforce efforts are due, in part, to the agency not viewing these challenges as a management priority. For example, as discussed earlier, the agency has not yet established time frames for completing key IT strategic planning activities, such as updating the strategic plan or workforce gap reviews. Until FEMA addresses these weaknesses, it will be difficult for the agency to ensure that its IT systems adequately support the ability to respond to major disasters.

None of the Three Selected Emergency Management Programs Had Fully Implemented Key IT Management Controls

The three selected major emergency management programs that we reviewed had not consistently implemented IT management controls in four key areas: (1) risk management, (2) requirements development, (3) project planning, and (4) systems integration and testing. For example, they had not always developed complete risk mitigation plans, ensured that stakeholders were adequately involved in identifying requirements, developed acquisition strategies or maintained cost and schedule estimates, and developed plans for integrating and testing system components. These weaknesses stemmed in part from gaps in FEMA policy for implementing these controls. As a result, the agency has less assurance that its emergency management systems, once delivered, will be within cost and schedule parameters and that current systems meet the capabilities needed by its users.

Programs Have Identified Key Risks, but Are Not Adequately Mitigating Them

According to the Software Engineering Institute's Capability Maturity Model Integration for Acquisition (CMMI-ACQ) and the PMBOK® Guide, an effective risk management process identifies potential problems before they occur, so that risk-handling activities may be planned and invoked as needed across the life of the project in order to mitigate adverse impacts on achieving objectives. Specifically, key risk management practices include

- identifying risks, threats, and vulnerabilities that could negatively affect work efforts;
- evaluating and categorizing each identified risk using defined risk categories and parameters, such as likelihood and consequence, and determining each risk's relative priority;
- developing risk mitigation plans and milestones for key mitigation deliverables for selected risks to proactively reduce the potential impact of risk occurrence, which includes a period of performance, identification of resources needed, and responsible parties; and
- monitoring the status of each risk periodically and implementing the risk mitigation plan as appropriate.

While all three programs had fully identified and evaluated key risks, none of the programs had developed adequate mitigation plans, and only one was fully monitoring risks' status. Table 1 provides a summary of the status of the three programs' implementation of key risk management

activities. Additional details on each program's implementation of these practices are provided below the table.

Table 1: Selected Federal Emergency Management Agency Programs' Implementation of Key Risk Management Practices

Risk management practice	DAIP	EMMIE	IPAWS
Identifying risks, threats, and vulnerabilities that could negatively affect work efforts	Fully implemented	Fully implemented	Fully implemented
Evaluating and categorizing each identified risk using defined risk categories and parameters	Fully implemented	Fully implemented	Fully implemented
Developing risk mitigation plans for selected risks	Partially implemented	Partially implemented	Partially implemented
Monitoring the status of each risk periodically and implementing the risk mitigation plan as appropriate	Partially implemented	Partially implemented	Fully implemented

Fully implemented Fully implemented: The agency provided evidence that it fully addressed this practice.

Partially implemented Partially implemented: The agency provided evidence that it addressed some, but not all, portions of this practice.

Not implemented Not implemented: The agency did not provide any evidence that it addressed this practice.

DAIP=Disaster Assistance Improvement Program

EMMIE=Emergency Management Mission Integrated Environment

IPAWS=Integrated Public Alert and Warning System

Source: GAO analysis of agency data. | GAO-16-306

- **DAIP**: The DAIP Program Office identified risks, threats, and vulnerabilities that could negatively affect work efforts in its risk register, including risks related to schedule and technology. For example, a key risk identified by the program's August 2015 risk register was not having participation from key security stakeholders in the integrated project teams, which could result in not receiving early feedback to inform the proposed solution. This could lead to either a delay in the design and progression of the solutions or the team having to spend time and money heading down a path that will not be approved.

  The program office also evaluated and categorized each identified risk using defined risk categories and parameters, such as likelihood and consequence, and determined each risk's relative priority. For example, the program office reported that the key risk mentioned above had a high probability of occurrence, high scope impact, high schedule impact, and medium cost impact, thus resulting in a high priority level.

Nonetheless, the program office did not develop adequate risk mitigation plans for selected risks to proactively reduce the potential impact of their occurrence. For example, the risk mitigation plan described the overall mitigation action and who was responsible, but did not include details on what, when, and how it will be done to avoid the risk or minimize consequences if the risk becomes a liability. As an example, for the key risk previously mentioned, the mitigation plan was for the program management office to work to engage and obtain committed participation from key security stakeholders, but additional details were not provided. Further, while the program office monitored each risk on a monthly basis, it could not demonstrate that it had implemented the risk mitigation plans as appropriate.

- **EMMIE:** The EMMIE program identified and analyzed risks by assigning a severity rating to risks and reviewing and evaluating these risks during monthly program risk management meetings. As of February 2016, the program office had identified four risks: (1) the test environment would not have needed capabilities, (2) the system does not have a backup or alternate processing site, (3) the system does not have a backup or alternative processing site, and (4) there are insufficient funds for cost estimates and the alternate processing site. For these risks, the program office also evaluated and categorized its risks based on probability and impact. For example, the program reported that the risks above had a “medium” exposure rating (meaning it may cause some increase in cost, disruption of schedule, or degradation of performance).

  However, the program office’s mitigation plans for identified risks were not adequate. For example, the risk mitigation action for the system backup states that there is planned migration of attachments into an enterprise-wide solution, but no details were provided on who will do this, what specifically will be done, or when and how it will be done to avoid the risk or minimize consequences if the risk becomes a liability. Further, while the program office monitored the risks on a monthly basis, it could not demonstrate that it implemented the risk mitigation plans as appropriate.

- **IPAWS:** The IPAWS program had identified risks, threats, and vulnerabilities that could negatively affect work efforts. For example, in August 2015, key risks identified by the program office included the lack of trained acquisition staff in the program office and the possibility of losing a private broadcast station due to industry action or natural

disaster, which could cause a major reduction in the ability to broadcast emergency alerts to the U.S. population.

The program office also evaluated and categorized its risks based on probability and impact. For example, the office reported that the training risk mentioned above has a high risk impact (meaning it can cause a high degree of cost overruns, schedule delays, and performance failures).

While IPAWS developed mitigation plans to reduce the potential impact of risk occurrence, they are not adequate. For example, risk mitigation plans for the two aforementioned key risks included escalating the issue to senior leadership to obtain staff for these positions and continuing outreach activities to industry partners, coordination with government entities, and emphasizing the benefits of services to the public. The plans did not include a period of performance or identification of resources needed, such as costs associated with implementing the plan. However, the program office monitors and reports on the status of each risk on a monthly basis, including the steps to be taken to mitigate the risks.

There is no FEMA guidance to assist programs in establishing a robust risk management process and OCIO officials acknowledged the weaknesses in this area. A robust process identifies potential problems before they occur, such as requiring programs to develop a risk management plan. Until the program offices and OCIO establish a risk management process that includes adequate risk mitigation plans and monitoring, they will lack assurance that they are properly managing all program risks.

Programs Did Not Ensure Requirements Were Well Defined

According to CMMI-ACQ and the PMBOK® Guide, appropriate requirements development involves eliciting and developing customer and stakeholder requirements, and analyzing them to ensure that they will meet users' needs and expectations. It also consists of validating requirements as the system is being developed to ensure that the final system to be deployed will perform as intended in an operational environment. Specifically, key risk requirements development practices include

- eliciting stakeholder needs, expectations, and constraints, and transforming them into prioritized customer requirements;
- developing and reviewing operational concepts and scenarios to refine and discover requirements;

- analyzing requirements to ensure that they are complete, feasible, and verifiable;
- analyzing requirements to balance stakeholder needs and constraints; and
- testing and validating the system as it is being developed.

The selected programs in our review varied in the degree to which they implemented the requirement practices. Table 2 provides a summary of the status of the three programs' implementation of key requirements development activities. Additional details on each program's implementation of these practices are provided below the table.

Table 2: Selected Federal Emergency Management Agency Programs' Implementation of Requirements Development Practices

Requirements management practices	DAIP	EMMIE	IPAWS
Eliciting stakeholder needs, expectations, and constraints, and transforming them into prioritized customer requirements	Partially implemented	Not implemented	Fully implemented
Developing and reviewing operational concepts and scenarios to refine and discover requirements	Not implemented	Not implemented	Fully implemented
Analyzing requirements to ensure that they are complete, feasible, and verifiable	Fully implemented	Not implemented	Fully implemented
Analyzing requirements to balance stakeholder needs and constraints	Partially implemented	Not implemented	Partially implemented
Testing and validating the system as it is being developed	Fully implemented	Fully implemented	Fully implemented

Fully implemented Fully implemented: The agency provided evidence that it fully addressed this practice.

Partially implemented Partially implemented: The agency provided evidence that it addressed some, but not all, portions of this practice.

Not implemented Not implemented: The agency did not provide any evidence that it addressed this practice.

DAIP=Disaster Assistance Improvement Program

EMMIE=Emergency Management Mission Integrated Environment

IPAWS=Integrated Public Alert and Warning System

Source: GAO analysis of agency data. | GAO-16-306

- **DAIP:** The program's contractor elicited stakeholder needs, expectations, and constraints, and transformed them into prioritized customer requirements. According to program officials, the program's Product Management and Project Management teams collaborate with contracted developers to perform requirements development and management activities using a backlog cataloging system. For example, changes to requirements are vetted through two different change control boards and backlog reviews, one conducted weekly at

the program level among program staff, and the other conducted bi-weekly in conjunction with all developer resources.

However, the program did not provide evidence that it completed operational concepts and scenarios to refine and discover requirements. Also, while the program analyzes requirements to ensure that they are complete, feasible, and verifiable by tracking them in a requirements traceability matrix, it has not provided evidence that it has analyzed requirements to balance stakeholder needs and constraints. For example, while, according to officials, DAIP has several mechanisms in place for analyzing requirements to balance stakeholder needs and constraints, including collecting and analyzing feedback from the users as to the functionality in the form of surveys, the program could not demonstrate that this was occurring.

Lastly, the program office tests and validates the system. For example, it performs and validates DAIP user acceptance testing to verify that requirements are met for systems.

- **EMMIE:** The program office lacked documentation to show that it had implemented the key requirement development activities. Specifically, according to program officials, much of the documentation, including plans and policies for developing and managing requirements, was not completed because the program was originally a task order to an existing contract. For example, while program officials stated that initial requirements were validated by user representatives designated by FEMA's Public Assistance program, there was no evidence of this. Additionally, the program office did not trace each requirement in a requirements traceability matrix to the program's desired capabilities and technical baselines.

  Program officials stated that, in the absence of a requirements management process, the EMMIE Program Manager works with program leadership to prioritize additional functionality or other changes to the system, translate those requests into change requests, and manage the delivery of requested changes by the EMMIE contractor. For example, according to EMMIE officials, ongoing requirements are validated on a bi-weekly basis by user groups compromised of representatives from FEMA headquarters and each of the 10 regions. Furthermore, FEMA officials stated that the agency performs annual reviews with the contractor to evaluate the operational results, but documentation is not available because it is not a written review. However, the program office did provide evidence that testing and validating of the system was completed as it

was being developed. Nonetheless, without documenting critical requirements development activities, the agency lacks assurance that EMMIE meets the needs of the users.

- **IPAWS:** The program office had obtained stakeholder needs and expectations and translated them into draft customer requirements. Specifically, the office compiled and drafted the emergency alert requirements from various executive orders, presidential memoranda, and laws. Additionally, the office developed operational concepts and scenarios to refine and discover requirements and analyze requirements to ensure they are complete, feasible, and verifiable. For example, it developed a Concept of Operations that included, among other things, a description of the environment in which the program will operate, including boundaries and constrains, and scenarios, such as the mission support and functional capabilities scenarios. The program office also analyzed requirements to make sure they were complete, feasible, and verifiable. For example, requirements and changes to requirements were discussed in monthly change control board meetings.

  The IPAWS program office did not fully analyze requirements to balance stakeholder needs and constraints. For example, it did not complete key steps to analyze IPAWS requirements, including performing a risk assessment on requirements and design constraints and did not perform a cost-benefit analysis to assess the impact of the requirements on the overall acquisition strategy. However, the program office had tested and evaluated the system as it was being developed. Specifically, the office had a test plan and test cases to determine whether the system was working as intended.

According to all three program offices and OCIO officials, FEMA policy guidance for requirements management does not exist. Given the lack of guidance, program offices' cannot implement effective requirements management practices. Without it, FEMA lacks assurance that these programs are delivering systems that will provide functionality that meets users' needs.

Program Offices Did Not Adequately Maintain Project Plans or Cost and Schedule Estimates

According to CMMI-ACQ, the PMBOK® Guide, and our prior work, an effective project planning process establishes project objectives and outlines the course of action required to attain those objectives. It also provides a means to track, review, and report progress and performance of the project by defining project activities and developing cost and

schedule estimates, among other things. Key activities in planning the program include

- establishing and maintaining the program's acquisition strategy;
- developing and maintaining the overall project plan, and obtaining commitment from relevant stakeholders;
- developing and maintaining the program's cost estimate;
- establishing and maintaining the program's schedule estimate; and
- identifying the necessary knowledge and skills needed to carry out the program.

The three selected programs varied in the extent to which they implemented these practices. For example, while IPAWS had developed and maintained acquisition strategies, DAIP and EMMIE had not. Additionally, all three programs had established a project plan, but did not regularly maintain it, and all three programs had developed cost estimates and schedules, but did not regularly maintain them.

Table 3 provides a summary of the status of the three programs' implementation of key project planning activities. Additional details on each program's implementation of these practices are provided below the table.

Table 3: Selected Federal Emergency Management Agency Programs' Implementation of Project Planning Practices

Project planning practice	DAIP	EMMIE	IPAWS
Establishing and maintaining the program's acquisition strategy	Partially implemented	Not implemented	Fully implemented
Developing and maintaining the overall project plan, and obtaining commitment from relevant stakeholders	Partially implemented	Partially implemented	Partially implemented
Developing and maintaining the program's cost estimate	Partially implemented	Partially implemented	Fully implemented
Establishing and maintaining the program's schedule estimate	Partially implemented	Partially implemented	Fully implemented
Identifying the necessary knowledge and skills needed to carry out the program	Not implemented	Not implemented	Not implemented

Fully implemented Fully implemented: The agency provided evidence that it fully addressed this practice.

Partially implemented Partially implemented: The agency provided evidence that it addressed some, but not all, portions of this practice.

Not implemented Not implemented: The agency did not provide any evidence that it addressed this practice.

DAIP=Disaster Assistance Improvement Program

EMMIE=Emergency Management Mission Integrated Environment

IPAWS=Integrated Public Alert and Warning System

Source: GAO analysis of agency data. | GAO-16-306

- **DAIP:** The DAIP Program Office established an acquisition strategy that identified the capabilities the program was intended to deliver, the acquisition approach, and objectives. Additionally, the DAIP program office developed an overall project plan that included the scope of the program, identified key program milestones, and obtained commitment from stakeholders. However, the program office had not updated the documents since September 2013 to reflect changing requirements.

  Further, it also developed a life-cycle cost estimate of about $240 million and a schedule estimate. However, neither the schedule nor the life-cycle cost estimate had been updated since September 2013. According to officials, the program is currently creating a cost estimating baseline document that will better inform its life-cycle cost estimate, which is expected to be completed in early spring 2016. Finally, the program plan did not identify the knowledge and skills needed to perform the project.

- **EMMIE:** According to program officials, an acquisition strategy for EMMIE was not developed. While the program office provided a draft project plan from April 2006 that included a cost estimate and schedule, it was not maintained on a regular basis. Additionally, while the life-cycle cost estimate for the program was about $28.3 million, the program office was unable to provide documentation on the total amount spent to date for EMMIE. Officials stated that it is difficult to identify the total amount spent to date for EMMIE because the total amount is spread across all Public Assistance grant systems rather than for EMMIE as a single system. Nonetheless, these officials stated that a reasonable estimate of total amount spent to date is about $22.7 million.

  Further, the program office could not demonstrate that it had obtained commitment from relevant stakeholders or identified the knowledge and skills needed to carry out the program. According to program officials, the Recovery Technology Program Division does not have a records repository for the EMMIE program and most key program documentation was not available, including the original program baseline, work orders related to EMMIE, or performance work statements.

- **IPAWS:** The IPAWS program had established and maintained an acquisition strategy. Specifically, the strategy identified the capabilities that the program is intended to deliver, the acquisition approach, and

the objectives of the acquisition. The IPAWS program also developed an overall project plan that included the scope of the program and identified key program milestones along with obtaining commitment from relevant stakeholders. However, the program office has not maintained the project plan since June 2010.

The program office did develop and maintain the program's cost estimate, and as of March 2015, the life-cycle cost estimate for IPAWS was $456 million. Similar to the program's cost estimate, IPAWS officials had developed and updated the program's schedule. According to program officials, they are reviewing the schedule, cost, and performance data on a monthly basis. However, the program plan did not identify the knowledge and skills needed to perform the project.

There is no FEMA guidance to assist program offices with project planning and OCIO officials acknowledged FEMA's weakness in this area. By not implementing the key activities of project planning, the program offices are not ensuring that the programs will be effectively implemented and managed going forward.

One Program Lacks Adequate Test Plans, and Two Programs Do Not Have Systems Integration Plans

Testing an IT system is essential to validate that the system will satisfy the requirements for its intended use and user needs. Best practices developed by the Institute of Electrical and Electronics Engineers (IEEE) recommend that systems testing should be conducted early and often in the life cycle of a systems development project to allow for the modification of products in a timely manner, thereby reducing the overall project and schedule impacts.[21] Additionally, according to CMMI-ACQ,[22] to ensure that all components of a system are appropriately integrated, a systems integration plan should be developed. Key activities for systems testing and integration include

- developing test plans and test cases that include a description of the overall approach for testing, identification of the test items that are the object of testing, the set of tasks necessary to prepare for and perform

[21]Institute of Electrical and Electronics Engineers, *IEEE Standard for Software and System Test Documentation,* IEEE Standard 829™ 2008 (New York, NY: July 18, 2008). All rights reserved.

[22]Software Engineering Institute, *Capability Maturity Model® Integration for Acquisition* (CMMI-ACQ), Version 1.3 (Pittsburgh, Pa.: November 2010).

testing, the roles and responsibilities for individuals or groups responsible for testing, the risk issues that may adversely impact successful completion of the planned testing activities, and the criteria to be used to determine whether each test item has passed or failed testing; and

- developing a systems integration plan to identify all systems to be integrated, define roles and responsibilities of all relevant participants, establish the sequence and schedule for every integration step, and describe how integration problems are to be documented and resolved.

The EMMIE and IPAWS program offices had developed adequate test plans and test cases, but only IPAWS had developed systems integration plans to ensure all systems to be integrated are identified and describe how integration problems are to be documented and resolved.

Table 4 provides a status of the three programs' implementation of key system testing and integration activities. Additional details on each program's implementation of these practices are provided below the table.

Table 4: Selected Federal Emergency Management Agency Programs' Implementation of Key System Testing and Integration Practices

System testing and integration practice	DAIP	EMMIE	IPAWS
Developing test plans and test cases	Partially implemented	Fully implemented	Fully implemented
Developing a systems integration plan	Not implemented	Not implemented	Fully implemented

Fully implemented Fully implemented: The agency provided evidence that it fully addressed this practice.

Partially implemented Partially implemented: The agency provided evidence that it addressed some, but not all, portions of this practice.

Not implemented Not implemented: The agency did not provide any evidence that it addressed this practice.

DAIP=Disaster Assistance Improvement Program

EMMIE=Emergency Management Mission Integrated Environment

IPAWS=Integrated Public Alert and Warning System

Source: GAO analysis of agency data. | GAO-16-306

- **DAIP:** The DAIP Program Office did not develop adequate test plans or prepare for system integration. Specifically, the program's test plans identified test items but did not identify roles and responsibilities for individuals or groups responsible for testing, and specify the criteria to be used to determine whether each test item has passed or failed testing.

Additionally, while program officials stated that about 15 systems interface with DAIP's assistance center, the program lacks a systems integration plan. According to program officials, one was not developed and DAIP was approved to operate without one in 2007. Officials stated that all system integration problems are tracked and analyzed by both FEMA and contractors to determine if they are new requirements or defects. For example, each item is further analyzed for the severity of the issue and a determination is made on how to most efficiently resolve it.

- **EMMIE:** The EMMIE program office tested and evaluated the system as it was being developed. Specifically, the program developed a testing plan that identifies the overall scope, method, and strategy to perform the testing. The plan also identifies the roles and responsibilities of the individuals responsible for testing. Furthermore, program officials stated that during testing, any deficiencies identified are captured as additional requirements. The Change Control Board, chaired by the Program Manager, reviews any requested changes and deficiencies on a bi-weekly basis.

  However, the program office did not develop a systems integration plan that includes all systems to be integrated, roles and responsibilities for all relevant participants, the sequence and schedule for every integration step, and how integration problems are to be documented and resolved. Officials stated that overall systems integration governance is described in the draft project management plan dated 2006, but this plan did not discuss, among other things, the strategy for system integration, environment needed to support the integration of the product components, or procedures and criteria for integration of the components. The program office also lacks documentation of the process associated with updating and maintaining the integration of the systems.

- **IPAWS:** The IPAWS program office tested and evaluated the system as it was being developed. Specifically, the office developed a testing plan that identifies the roles and responsibilities of the individuals responsible for testing. It also identifies the overall scope, method, and strategy to perform the testing. Further, IPAWS test cases included the necessary elements for a test case, such a unique identifier, which is used to identify each test case; specified object, inputs, and outputs; and the steps to take for the execution of the test. In addition, it identifies the necessary test environment and the criteria used to determine whether a test passed or failed. Furthermore, the

office developed an integration plan that includes key criteria, such as ensuring that component interfaces, both internal and external, are compatible.

Similar to the other selected IT controls, OCIO officials acknowledged that FEMA needs improvements in this area and there is no FEMA guidance on developing systems testing and integration plans. Without such plans, a risk exists that system testing will occur in an ad hoc and undisciplined fashion and the program offices will be limited in their ability to ensure that the resulting systems are integrated, functioning properly, and delivered on time and within budget to the users. Additionally, without a systems integration plan, the DAIP program is not ensuring that it is identifying all systems to be integrated and describing how integration problems are to be documented and resolved.

Conclusions

FEMA has acknowledged the urgency of modernizing its IT environment given the duplication and inefficiencies in its systems that agency officials have identified. However, the agency continues to face a number of challenges. Until the agency addresses shortcomings in its IT governance and oversight, strategic planning, and workforce planning, its progress is likely to be limited. Further, inconsistent implementation of key IT management controls calls into question how well FEMA is positioned to efficiently acquire major emergency management systems. Ensuring that these controls are fully implemented and reflected in agency policy will help FEMA deliver these systems on time and at an acceptable cost, and that they will provide needed capabilities to support the nation's emergency response efforts.

Recommendations for Executive Action

To ensure that FEMA's IT systems can adequately support its ability to respond to major disasters, we are recommending that the Secretary of DHS direct the FEMA Administrator to take the following actions:

- Ensure that the IT Governance Board has fully defined and implemented its roles and responsibilities for key boards, working groups, and individuals, and procedures for selecting and overseeing IT investments.
- Define the scope, implementation strategy, and schedule of the agency's overall modernization approach, with related goals and measures for effectively overseeing the effort. At a minimum, the

agency should update its IT strategic plan and complete its modernization plan.

- Establish time frames for current and future IT workforce planning during its modernization efforts and ensure all regions and offices are included in these initiatives.

To ensure that FEMA adequately manages the selected emergency management systems, we recommend that the FEMA Administrator direct the DAIP, EMMIE, and IPAWS program offices, in conjunction with the FEMA CIO, to implement

- a robust risk management process that identifies potential problems before they occur;
- a requirements management process to ensure requirements are well defined;
- complete program plans that define overall budget and schedule, key deliverables and milestones, assumptions and constraints, description and assignment of roles and responsibilities, staffing and training plans, and an approach for maintaining these plans; and
- a system integration plan that include all systems to be integrated with the system, roles and responsibilities for all relevant participants, the sequence and schedule for every integration step, and how integration problems are to be documented and resolved.
- As part of the effort of improving IT management at the three programs, we recommend that the FEMA Administrator direct the CIO to ensure that FEMA policy for managing IT programs includes guidance for implementing the key management practices.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from DHS's Director for the Departmental GAO-OIG Liaison Office. The comments are reprinted in appendix II.

In the comments, DHS concurred with our recommendations. In this regard, the Director described ongoing and planned actions to address the recommendations, and provided milestones for completing these actions. For example, the Director stated that the department plans to establish charters that clearly define roles and responsibilities, as well as procedures, standards, and guidelines for selection and management of

investments in the IT investment portfolio by December 31, 2016. Officials also provided technical comments, which we have incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees; the Secretary of the Department of Homeland Security, the Administrator of the Federal Emergency Management Agency; and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

Should you or your staff have any questions on information discussed in this report, please contact me at (202) 512-4456 or ChaC@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Carol R. Cha
Director, Information Technology Acquisition Management Issues

List of Requesters

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Michael T. McCaul
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Daniel Donovan
Chairman
The Honorable Donald M. Payne, Jr.
Ranking Member
Subcommittee on Emergency Preparedness, Response, and Communications
Committee on Homeland Security
House of Representatives

The Honorable Martha McSally
House of Representatives

The Honorable Susan W. Brooks
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) identify challenges associated with ensuring the Federal Emergency Management Agency's (FEMA) information technology (IT) systems adequately support the agency's ability to respond to major disasters and (2) assess the extent to which FEMA has implemented key IT management controls for selected emergency management systems.

To address our first objective, we obtained and analyzed FEMA documentation (e.g., FEMA's Hurricane Sandy After-Action Report), prior GAO reports, and Department of Homeland Security (DHS) inspector general (IG) reports. In addition, we interviewed officials from the National Advisory Council; the Disaster Emergency Communications Division; Regions 2, 4, and 6; the Mobile Emergency Response Center (Thomasville, Georgia); and the National Processing Center (Maryland). We selected Regions 2, 4, and 6 because, according to FEMA officials, these three regions contained the states that had the 10 most costly natural disasters since 2005. We also interviewed agency officials from FEMA's Office of the Chief Information Officer (OCIO), its Office of Policy & Program Analysis, and DHS's IG office to determine challenges associated with its IT systems. Subsequently, we identified three challenges that were identified by three or more sources and focused our review on FEMA's efforts to address them. These challenges were FEMA's (1) IT governance board, (2) IT modernization efforts, and (3) FEMA's IT workforce.

To determine the extent to which FEMA had adequate controls in place to address these challenges, we compared the agency's efforts to best practices we have identified in the areas of IT investment management,[1] human capital management,[2] and strategic planning.[3]

[1]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (Supersedes AIMD-10.1.23),* GAO-04-394G (Washington, D.C.: March 2004).

[2]GAO, *A Model of Strategic Human Capital Management,* GAO-02-373SP (Washington, D.C.: March 2002); *Human Capital: Key Principles for Effective Strategic Workforce Planning,* GAO-04-39 (Washington, D.C.: Dec. 11, 2003); and *Information Technology: FDA Needs to Establish Key Plans and Processes for Guiding Systems Modernization Efforts,* GAO-09-523 (Washington, D.C.: June 2, 2009).

[3]GAO, *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization*, GAO-12-495 (Washington, D.C.: Apr. 26, 2012).

Specifically, we compared the controls FEMA had in place to address the first challenge—the agency's IT governance board—against critical processes associated with Stage 2 of GAO's information technology investment management framework.[4] In particular, Stage 2 of the framework includes the following key processes for effective governance:

- instituting the investment board,
- selecting investments that meet business needs, and
- providing investment oversight.

For the second challenge—the agency's IT modernization efforts—we compared FEMA's controls to the best practices found in, among other sources, Office of Management and Budget guidance.[5] Those practices include

- developing a strategic plan that includes defining the agency's vision and providing a road map to help align information resources with business strategies and investment decisions.

Lastly, for the third challenge—IT workforce—we compared FEMA's IT management controls to GAO's A Model of Strategic Human Capital Management and the Office of Personnel Management's Human Capital Assessment and Accountability Framework.[6] Those practices include

- analyzing the gaps between current skills and future needs and
- developing strategies for filling the gaps.

For the second objective, we used the following criteria to select three programs to review:

- The program was associated with objectives of the systems identified in the Post-Katrina Emergency Management Reform Act of 2006.

[4]GAO-04-394G.

[5]OMB, *Guidance on Exhibits 53 and 300 – Information Technology and E-Government* (Washington, D.C.: July 1, 2013).

[6]GAO-02-373SP and Office of Personnel Management, *Human Capital Assessment and Accountability Framework—Systems, Standards, and Metrics* (http://www.opm.gov/hcaaf_resource_center/).

- At least one program must have been identified as a major IT investment, as defined by the Office of Management and Budget.[7]
- The program must have planned spending in fiscal year 2015.
- The program must be disaster-related.
- The program must not be fully deployed or have been recently approved for termination.
- The program must not have been included in a recent GAO or IG review that examined the program's IT management controls.

Using the above criteria, we selected the following three programs:

1. Disaster Assistance Improvement Program (DAIP): A major system used for conducting phone and web surveys with FEMA external customers and internal personnel.
2. Emergency Management Mission Integrated Environment (EMMIE): An Internet-based enterprise-wide electronic system to manage grants throughout their entire life cycle using a standardized web-based interface.
3. Integrated Public Alert & Warning System (IPAWS): A major system that provides a broad range of messaging capabilities through multiple pathways to ensure the delivery of alerts and warnings reaches more people, more reliably, increasing resilience of local systems to ensure operational readiness.

We then determined the extent to which the three selected programs identified above were implementing key IT acquisition practices in the areas of risk management, requirements management, project planning, and systems integration and testing. We selected these key IT management control areas because they are consistent with the requirements of the Post-Katrina Act[8] for FEMA to take steps to improve its IT systems, including:

[7]The Office of Management and Budget defines a major IT investment as a system or an acquisition requiring special management attention because it has significant importance to the mission or function of the agency, a component of the agency, or another organization; is for financial management and obligates more than $500,000 annually; has significant program or policy implications; has high executive visibility; has high development, operating, or maintenance costs; is funded through other than direct appropriations; or is defined as major by the agency's capital planning and investment control process.

[8]Post-Katrina Act, Title VI, Pul,L. No. 109-295, sec.640 (2006); 6 U.S.C. § 727.

- ensuring that the information technology systems of the agency have the capacity to track disaster response personnel, mission assignments task orders, commodities, and supplies used in response to a natural disaster, act of terrorism, or other man-made disaster;
- ensuring that the multiple IT systems of the agency are, to the extent practicable, fully compatible and can share and access information, as appropriate, from each other;
- ensuring technology enhancements reach the headquarters and regional offices of the agency in a timely fashion, to allow seamless integration; and
- developing and maintaining a testing environment that ensures that all system components are properly and thoroughly tested before their release.

To determine the extent to which the three programs implemented IT management controls, we reviewed documentation from the three selected programs and compared it to key management best practices, including the Software Engineering Institute's Capability Maturity Model® Integration for Acquisition (CMMI-ACQ) and the Project Management Institute's Guide to the Project Management Body of Knowledge (PMBOK® Guide).[9] We assessed the program as having implemented a practice if the agency provided evidence that it fully addressed this practice, partially implemented if the agency provided evidence that it addressed some, but not all, portions of this practice, and not implemented if the agency did not provide any evidence that it addressed this practice.

In particular, the key risk management best practices were

- identifying risks, threats, and vulnerabilities that could negatively affect work efforts;

[9]Software Engineering Institute, *Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3* (Pittsburgh, Pa.: November 2010); Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Fifth Edition,* (Newton Square, Pa.: 2013).

- evaluating and categorizing each identified risk using defined risk categories and parameters, such as likelihood and consequence, and determining each risk's relative priority;
- developing risk mitigation plans for selected risks to proactively reduce the potential impact of risk occurrence; and
- monitoring the status of each risk periodically and implementing the risk mitigation plan as appropriate.

The key requirements development best practices were

- eliciting stakeholder needs, expectations, and constraints, and transforming them into prioritized customer requirements;
- developing and reviewing operational concepts and scenarios to refine and discover requirements;
- analyzing requirements to ensure that they are complete, feasible, and verifiable;
- analyzing requirements to balance stakeholder needs and constraints; and
- testing and validating the system as it is being developed.

The key project planning best practices were

- establishing and maintaining the program's acquisition strategy;
- developing and maintaining the overall project plan, and obtaining commitment from relevant stakeholders;
- developing and maintaining the program's cost estimate;
- establishing and maintaining the program's schedule estimate; and
- identifying the necessary knowledge and skills needed to carry out the program.

Lastly, the key systems testing and integration best practices were

- developing test plans and test cases; and

- developing a systems integration plan to identify all systems to be integrated.

To determine the status of each program's key risks and the actions that were taken to manage these risks, we analyzed program risk documentation, including monthly risk logs and reports, risk management plans, and risk mitigation plans. For requirements development, we analyzed monthly program management review briefings, business cases, acquisition strategies, concepts of operations, and system requirements documentation. For project planning, we analyzed project plans, business cases, acquisition strategies, master schedules, and life-cycle cost estimates. For systems testing and integration, we analyzed testing strategies, test execution plans, change control board meeting minutes and test cases. Additionally, we interviewed program officials to obtain additional information on each program's management control practices.

To assess the reliability of the data that we used to support the findings in this report, we corroborated relevant program documentation and interviews with agency officials. We determined that the data used in this report were sufficiently reliable.

We conducted this performance audit from January 2015 to April 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

March 17, 2016

Carol R. Cha
Director, Information Technology Acquisition Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-16-306, "INFORMATION TECHNOLOGY: FEMA Needs to Address Management Weaknesses to Improve Its Systems."

Dear Ms. Cha:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this draft report.

The Department is pleased to note GAO's positive recognition of the Federal Emergency Management Agency's (FEMA) efforts to modernize its information technology (IT) environment by beginning to address the practices essential to having a solid foundation for sound, information technology investment processes. These practices will help FEMA attain successful, predictable, and repeatable investment control processes at the project level. FEMA is committed to ensuring that its IT programs adequately support the ability to respond to major disasters, and is doing this by delivering on the commitment in the Modernization Plan, as well as the planning and execution of the IT Management Framework and IT Management Plan.

Establishing an IT Management Framework that integrates federal mandates and IT management best practices into a seamless system of management procedures will provide transparency, accountability, and responsibility to the project life cycle and move FEMA forward. Enhancing IT investment management processes based on the foundations of capital planning and investment control (CPIC) will allow FEMA to deliver IT systems that can better support its response to major disasters.

The draft report contained eight recommendations with which the Department concurs. Specifically, GAO recommended that the Secretary of DHS direct the FEMA Administrator to take the following actions:

Recommendation 1: Ensure that the IT Governance Board has fully defined and implemented its roles and responsibilities for key boards, working groups and individuals, and procedures in selecting and overseeing IT investments.

Response: Concur. FEMA's IT Governance Board (ITGB) serves as the primary structure for IT decision-making. To mature IT governance, FEMA will integrate other governing bodies to formalize a comprehensive governance structure for IT decisions that leverages work performed across various levels of the Agency in the management of investments and technology. FEMA will establish charters that clearly define roles and responsibilities; as well as procedures, standards, and guidelines for selection and management of investments in the IT Investment Portfolio. Estimated Completion Date (ECD): December 31, 2016

Recommendation 2: Define the scope, implementation strategy, and schedule of its overall modernization approach, with related goals and measures for effectively overseeing the effort. At a minimum, the agency should update its IT strategic plan and complete its modernization plan.

Response: Concur. FEMA will take the following three actions:

Action 1. FEMA published its IT Strategic Plan in FY 2012 that addressed FEMA IT strategy from FY 2012 – FY 2017, establishing six goals that support execution of the FEMA FY 2014 – FY 2018 Strategic Plan. FEMA will reevaluate the IT strategies in the current plan and make any adjustments necessary to meet FEMA's goals and objectives before issuing an extension to the IT Strategic Plan to be effective through FY 2020. Upon completion of the FEMA FY 2019 – FY 2023 Strategic Plan, FEMA will engage in a detailed assessment of progress made from implementation of the IT Modernization Plan and changes in business drivers specified in the new Agency Strategy Plan to establish a FY 2021 – FY 2026 IT Strategic Plan. This assessment will enable FEMA to better align future planning efforts between the Agency Strategic Plan and the IT Strategic Plan. FEMA will modify the current IT Strategic Plan, as appropriate after detailed analysis, and extend the plan to FY 2020 by October 31, 2016.

Action 2. FEMA leveraged the findings from the IT Resiliency Review and Cyber Sprint activities conducted in 2015, as well as the goals from the IT Strategic Plan, to develop a cohesive five year IT Modernization Plan. This plan identifies functional capabilities and IT program management maturity requirements for executing FEMA's IT strategic goals and objectives. The draft IT Modernization Plan was completed in December 2015 and is now in the final stages of Executive Review before it is forwarded to DHS. Implementation of this plan will be a collaborative and transparent partnership between

2

DHS's Office of the Chief Information Officer (OCIO), FEMA mission areas, Regions, and our state, local, Tribal, private sector, and non-governmental partners. FEMA will formally submit the IT Modernization Plan to DHS by April 30, 2016.

Action 3. FEMA is now beginning the efforts to guide in-depth, cross-functional work sessions by reviewing the investments identified in the Modernization Plan to establish an actionable implementation roadmap. This implementation roadmap will be in line with Agency priorities based on business drivers and Agency capacity; best practices to reduce duplication of infrastructure and capabilities; reconciling interdependencies across the portfolio; aligning funding to accomplish priorities; and assigning adequately staffed and skilled, integrated project teams to plan and manage the projects in accordance with Agency guidelines. ECD: November 30, 2016.

Recommendation 3: Establish time frames for current and future IT workforce planning during its modernization efforts and ensure all regions and offices are included in these initiatives.

Response: Concur. FEMA will take the following two actions:

Action 1. As part of the implementation planning workshops, with all Agency offices and regions, FEMA will align priorities and resources to establish adequately staffed integrated project teams responsible for the successful execution of modernization projects.

Action 2. FEMA will complete an IT workforce utilization review to identify specific skill gaps in supporting the Agencies' IT projects, systems, and services. This review will facilitate the alignment of skilled staff within functional groups, determine sourcing strategy to fill shortfalls, and establish development plans to prepare staff to lead and support the direction of FEMA's IT program. ECD: November 30, 2016.

Recommendation 4: To ensure that FEMA adequately manages the selected emergency management systems, we recommend that the FEMA Administrator direct the DAIP [Disaster Assistance Improvement Plan], EMMIE [Emergency Management Mission Integrated Environment], EMMIE [Integrated Public Alert and Warning System] program offices, in conjunction with the FEMA CIO, to implement a robust risk management process that identifies potential problems before they occur.

Response: Concur. To ensure adequate management of DAIP, EMMIE, and IPAWS, FEMA OCIO will work with the Program Offices to develop a robust risk management plan that identifies the process of identifying, analyzing and responding to risk factors throughout the life of each project to proactively address potential issues before they become problematic. ECD: June 30, 2016.

3

Recommendation 5: To ensure that FEMA adequately manages the selected emergency management systems, we recommend that the FEMA Administrator direct the DAIP, EMMIE, and IPAWS program offices, in conjunction with the FEMA CIO, to implement a requirements management process to ensure requirements are well defined.

Response: Concur. FEMA's OCIO will work with Program Offices to develop a requirements management plan that identifies a common understanding of how business, functional, and technical requirements will be identified, analyzed, documented, and managed for each project. ECD: June 30, 2016.

Recommendation 6: To ensure that FEMA adequately manages the selected emergency management systems, we recommend that the FEMA Administrator direct the DAIP, EMMIE, and IPAWS program offices, in conjunction with the FEMA CIO, to implement complete program plans that define overall budget and schedule, key deliverables and milestones, assumptions and constraints, description and assignment of roles and responsibilities, staffing and training plans, and an approach for maintaining these plans.

Response: Concur. FEMA's OCIO will work with Program Offices to develop a program management plan to identify and describe the overall program management processes and methods to be used during all phases of the projects that defines overall budget and schedule, key deliverables and milestones, assumptions and constraints, description and assignment of roles and responsibilities, staffing and training plans, and an approach for maintaining these plans. ECD: June 30, 2016.

Recommendation 7: To ensure that FEMA adequately manages the selected emergency management systems, we recommend that the FEMA Administrator direct the DAIP, EMMIE, and IPAWS program offices, in conjunction with the FEMA CIO, to implement a system integration plan that include all systems to be integrated with the system, roles and responsibilities for all relevant participants, the sequence and schedule for every integration step, and how integration problems are to be documented and resolved.

Response: Concur. FEMA's OCIO will work with Program Offices to develop a systems integration plan that provides an overview of each base system, a listing of all existing systems impacted by the system interfaces, and a description of what components are integrated at each step, with a description of the major tasks involved in the integration, and the overall resources needed to support the integration effort. ECD: August 31, 2016.

Recommendation 8: As part of the effort of improving IT management at the three programs, direct the CIO to ensure that FEMA policy for managing IT programs includes guidance for implementing the key management practices.

4

Response: Concur. FEMA's OCIO will review and update the FEMA policy for managing IT programs to include guidance for implementing the key management practices. ECD: September 30, 2016

Again, thank you for the opportunity to comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

5

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Carol R. Cha at (202) 512-4456 or ChaC@gao.gov

Staff Acknowledgments

In addition to the contact name above, the following staff also made key contributions to this report: Eric Winter (Assistant Director), Chris Businsky, Lee McCracken, Tyler Mountjoy, Kate Nielsen, Teresa Smith, and Niti Tandon.

Appendix IV: Accessible Data

Agency Comments

Text of Appendix II: Comments from the Department of Homeland Security

Page 1

March 17, 2016

Carol R. Cha

Director, Information Technology Acquisition Management Issues

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Re: Draft Report GA0-16-306, "INFORMATION TECHNOLOGY: FEMA

Needs to Address Management Weaknesses to Improve Its Systems."
Dear Ms. Cha:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this draft report.

The Department is pleased to note GAO's positive recognition of the Federal Emergency Management Agency's (FEMA) efforts to modernize its information technology (IT) environment by beginning to address the practices essential to having a solid foundation for sound, information technology investment processes. These practices will help FEMA attain successful, predictable, and repeatable investment control processes at the project level. FEMA is committed to ensuring that its IT programs adequately support the ability to respond to major disasters, and is doing this by delivering on the commitment in the Modernization Plan, as well as the planning and execution of the IT Management Framework and IT Management Plan.

Establishing an IT Management Framework that integrates federal mandates and IT management best practices into a seamless system of management procedures will provide transparency, accountability, and responsibility to the project life cycle and move FEMA forward. Enhancing IT investment management processes based on the foundations of capital planning and investment control (CPIC) will allow

FEMA to deliver IT systems that can better support its response to major disasters.

Page 2

The draft report contained eight recommendations with which the Department concurs. Specifically, GAO recommended that the Secretary of DHS direct the FEMA Administrator to take the following actions:

Recommendation 1:

Ensure that the IT Governance Board has fully defined and implemented its roles and responsibilities for key boards, working groups and individuals, and procedures in selecting and overseeing IT investments.

Response: Concur.

FEMA's IT Governance Board (ITGB) serves as the primary structure for IT decision-making. To mature IT governance, FEMA will integrate other governing bodies to fonnalize a comprehensive governance structure for IT decisions that leverages work performed across various levels of the Agency in the management of investments and technology. FEMA will establish charters that clearly define roles and responsibilities; as well as procedures, standards, and guidelines for selection and management of investments in the IT Investment Portfolio. Estimated Completion Date (ECD): December 31, 2016

Recommendation 2:

Define the scope, implementation strategy, and schedule of its overall modernization approach, with related goals and measures for effectively. overseeing the effort. At a minimum, the agency should update its IT strategic plan and complete its modernization plan.

Response: Concur.

FEMA will take the following three actions:

Action 1.

FEMA published its IT Strategic Plan in FY 2012 that addressed FEMA IT strategy from FY 2012 -FY 2017, establishing six goals that support execution of the FEMA FY 2014 -FY 2018 Strategic Plan. FEMA will reevaluate the IT strategies in the current plan and make any adjustments necessary to meet FEMA's goals and objectives before issuing an extension to the IT Strategic Plan to be effective through FY 2020.

Upon completion of the FEMA FY 2019 -FY 2023 Strategic Plan, FEMA will engage in a detailed assessment of progress made from implementation of the IT Modernization Plan and changes in business drivers specified in the new Agency Strategy Plan to establish a FY 2021 -FY 2026 IT Strategic Plan. This assessment will enable FEMA to better align future planning efforts between the Agency Strategic Plan and the IT Strategic Plan. FEMA will modify the current IT Strategic Plan, as appropriate after detailed analysis, and extend the plan to FY 2020 by October 31, 2016.

Action 2.

FEMA leveraged the findings from the IT Resiliency Review and Cyber Sprint activities conducted in 2015, as well as the goals from the IT Strategic Plan, to develop a cohesive five year IT Modernization Plan. This plan identifies functional capabilities and IT program management maturity requirements for executing FEMA' s IT strategic goals and objectives. The draft IT Modernization Plan was completed in December 2015 and is now in the final stages of Executive Review before it is forwarded to DHS. Implementation of this plan will be a collaborative and transparent partnership between

Page 3

DHS's Office of the Chief Information Officer (OCIO), FEMA mission areas, Regions, and our state, local, Tribal, private sector, and non-governmental partners. FEMA will formally submit the IT Modernization Plan to DRS by April 30, 2016.

Action 3.

FEMA is now beginning the efforts to guide in-depth, cross-functional work sessions by reviewing the investments identified in the Modernization Plan to establish an actionable implementation roadmap. This implementation roadmap will be in line with Agency priorities based on business drivers and Agency capacity; best practices to reduce

duplication of infrastructure and capabilities; reconciling interdependencies across the portfolio; aligning funding to accomplish priorities; and assigning adequately staffed and skilled, integrated project teams to plan and manage the projects in accordance with Agency guidelines. ECD: November 30, 2016.

Recommendation 3:

Establish time frames for current and future IT workforce planning during its modernization efforts and ensure all regions and offices are included in these initiatives.

Response: Concur.

FEMA will take the following two actions:

Action 1.

As part of the implementation planning workshops, with all Agency offices and regions, FEMA will align priorities and resources to establish adequately staffed integrated -project teams responsible for the successful execution of modernization projects.

Action 2.

FEMA will complete an IT workforce utilization review to identify specific skill gaps in supporting the Agencies' IT projects, systems, and services. This review will facilitate the alignment of skilled staff within functional groups, determine sourcing strategy to fill shortfalls, and establish development plans to prepare staff to lead and support the direction of FEMA's IT program. ECD: November 30, 2016.

Recommendation 4:

To ensure that FEMA adequately manages the selected emergency management systems, we recommend that the FEMA Administrator direct the DAIP [Disaster Assistance Improvement Plan], EMMIE [Emergency Management Mission. Integrated Environment], EMMIE [Integrated Public Alert and Warning System] program offices, in conjunction with the FEMA CIO, to implement a robust risk management process that identifies potential problems before they occur.

Response: Concur.

To ensure adequate management of DAIP, EMMIE, and IPAWS, FEMA OCIO will work with the Program Offices to develop a robust risk management plan that identifies the process of identifying, analyzing and responding to risk factors throughout the life of each project to proactively address potential issues before they become problematic. ECD: June 30, 2016.

Page 4

Recommendation 5:

To ensure that FEMA adequately manages the selected emergency management systems, we recommend that the FEMA Administrator direct the DAIP, EMMIE, and IPAWS program offices, in conjunction with the FEMA CIO, to inplement a requirements management process to ensure requirements are well defined.

Response: Concur.

FEMA's OCIO will work with Program Offices to develop a requirements management plan that identifies a common understanding of how business, functional, and technical requirements will be identified, analyzed, documented, and managed for each project. ECD: June 30, 2016.

Recommendation 6:

To ensure that FEMA adequately manages the selected emergency management systems, we recommend that the FEMA Administrator direct the DAIP, EMMIE, and IPAWS program offices, in conjunction with the FEMA CIO, to implement complete program plans that define overall budget and schedule, key deliverables and milestones, assumptions and constraints, description and assignment of roles and responsibilities, staffing and training plans, and an approach for maintaining these plans.

Response: Concur.

FEMA's OCIO will work with Program Offices to develop a program management plan to identify and describe the overall program management processes and methods to be used during all phases of the projects that defines overall budget and schedule, key deliverables and milestones, assumptions and constraints, description and assignment of

roles and responsibilities, staffing and training plans, and an approach for maintaining these plans. ECD: June 30, 2016.

Recommendation 7:

To ensure that FEMA adequately manages the selected emergency management systems, we recommend that the FEMA Administrator direct the DAIP, EMMIE, and IPAWS program offices, in conjunction with the FEMA CIO, to implement a system integration plan that include all systems to be integrated with the system, roles and responsibilities for all relevant participants, the sequence and schedule for every integration step, and how integration problems are to be documented and resolved.

Response: Concur.

FEMA's OCIO will work with Program Offices to develop a systems integration plan that provides an overview of each base system, a listing of all existing systems impacted by the system interfaces, and a description of what components are integrated at each step, with a description of the major tasks involved in the integration, and the overall resources needed to support the integration effort. ECD: August 31, 2016.

Recommendation 8:

As part of the effort of improving IT management at the three programs, direct the CIO to ensure that FEMA policy for managing IT programs includes guidance for implementing the key management practices.

Page 5

Response: Concur.

FEMA's OCIO will review and update the FEMA policy for managing IT programs to include guidance for implementing the key management practices. ECD: September 30, 2016

Again, thank you for the opportunity to comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

H. Crumpac cer, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548