

FEMA Faces Challenges in Managing Information Technology





DHS OIG HIGHLIGHTS

FEMA Faces Challenges in Managing Information Technology

November 20, 2015

Why We Did This Audit

In a 2011 audit, we reported challenges in FEMA's information technology (IT) management and infrastructure. We conducted this follow-up audit to determine whether FEMA's current IT management approach adequately addresses the technology planning, governance, and system challenges to support its mission.

What We Recommend

We made five recommendations to the FEMA Chief Information Officer to improve planning, governance, and management of technology to support FEMA's mission.

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The Federal Emergency Management Agency (FEMA) has taken steps to improve its IT management since our 2011 audit, but more remains to be done. Specifically, FEMA has developed numerous IT planning documents but has not effectively coordinated, executed, or followed through on these plans. Without effective IT planning, FEMA risks making limited progress improving IT needed to support the agency's mission. Although FEMA has improved its IT governance through establishing an IT Governance Board, these efforts have not yet been fully effective.

FEMA has struggled to implement effective agency-wide IT governance, in part because the Chief Information Officer has not had sufficient control and budget authority to effectively lead the agency's decentralized IT environment. Without effective agency-wide IT governance, FEMA's IT environment has evolved over time to become overly complex, difficult to secure, and costly to maintain.

Further, in this complex, decentralized IT environment, FEMA's IT systems are not sufficiently integrated and do not provide personnel with the data search and reporting tools they need. As a result of system limitations, end users engage in inefficient, time-consuming business practices that can increase the risk that disaster assistance and grants could be delayed and duplication of benefits could occur.

FEMA Response

FEMA concurred with our recommendations.



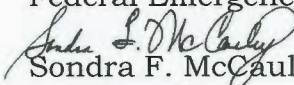
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

November 20, 2015

MEMORANDUM FOR: Adrian Gardner
Chief Information Officer
Federal Emergency Management Agency

FROM: 
Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *FEMA Faces Challenges in Managing Information Technology*

Attached for your action is our final report, *FEMA Faces Challenges in Managing Information Technology*. We incorporated the formal comments provided by your office.

The report contains five recommendations aimed at improving FEMA's management of information technology. Your office concurred with all five recommendations. Based on information provided in your response to the draft report, we consider recommendations 1, 2, 4, and 5 resolved and open. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Recommendation 3 is resolved and closed.

Please send your response or closure request to OIGITAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Steven Staats, Audit Manager, at (202) 254-4224.

Attachment



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Table of Contents

Background	3
Results of Audit	7
IT Planning Progress and Challenges	7
Effective IT Governance Has Not Yet Been Fully Established	14
IT Systems Do Not Fully Support Mission Needs	19

Appendixes

Appendix A: Objective, Scope, and Methodology	26
Appendix B: FEMA Comments to the Draft Report	28
Appendix C: Office of Information Technology Audits Major Contributors to This Report	32
Appendix D: Report Distribution	33

Abbreviations

CIO	Chief Information Officer
DHS	Department of Homeland Security
eCAPS	Enterprise Coordination and Approval Processing System
eGrants	Mitigation Electronic Grants
EMMIE	Emergency Management Mission Integration Environment
FEMA	Federal Emergency Management Agency
FY	fiscal year
GAO	Government Accountability Office
IT	information technology
ITGB	IT Governance Board
ND-Grants	Non-Disaster Grants Management System
NEMIS	National Emergency Management Information System
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
WebEOC	Web-based Emergency Operations Center
WebIFMIS	Web Integrated Financial Management Information System



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

The Federal Emergency Management Agency (FEMA) coordinates the Federal government's activities to prepare for, prevent, mitigate the effects of, respond to, and recover from all domestic disasters, whether natural or man-made, including acts of terror. FEMA's authority is derived from the *Disaster Relief Act of 1974*, as amended by the *Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988*.¹

To accomplish its mission, FEMA has approximately 18,450 government employees and contractors working at its headquarters offices in Washington, DC, as well as 10 regional offices, 3 area offices, and various temporary disaster-related sites that carry out FEMA's operations throughout the United States and its territories. Additionally, FEMA has more than 7,000 employees who remain on standby for deployment during disasters. It partners with other Federal, state, tribal, and local emergency management agencies; non-governmental and private sector agencies; and various community-based participants that also have disaster response and recovery responsibilities. For fiscal year (FY) 2015, FEMA's budget request was approximately \$14.7 billion, representing 24 percent of the Department of Homeland Security's (DHS) budget request of approximately \$60.9 billion.

FEMA's primary mission areas include:

- Federal Insurance and Mitigation Administration – manages the National Flood Insurance Program and a range of programs designed to reduce future losses from natural disasters.
- Protection and National Preparedness – coordinates preparedness and protection-related activities throughout FEMA, including grants, planning, training, exercises, individual and community preparedness, and national capital region coordination.
- Response and Recovery – coordinates Federal operational and logistical disaster response capabilities to save and sustain lives, minimize suffering, and protect property in a timely and effective manner in communities overwhelmed by disasters. Individual and public assistance programs, as well as long-term community recovery efforts support FEMA's efforts to prepare for, respond to, and recover from all hazards.
- United States Fire Administration – provides national leadership for fire and emergency services stakeholders by providing training programs and conducting research on fire detection, prevention, and suppression, as well as first responder health, safety, and effectiveness.
- Regional Operations – ensures effective coordination between headquarters and regional offices.

¹ Public Laws 93-288 and 100-707, respectively.



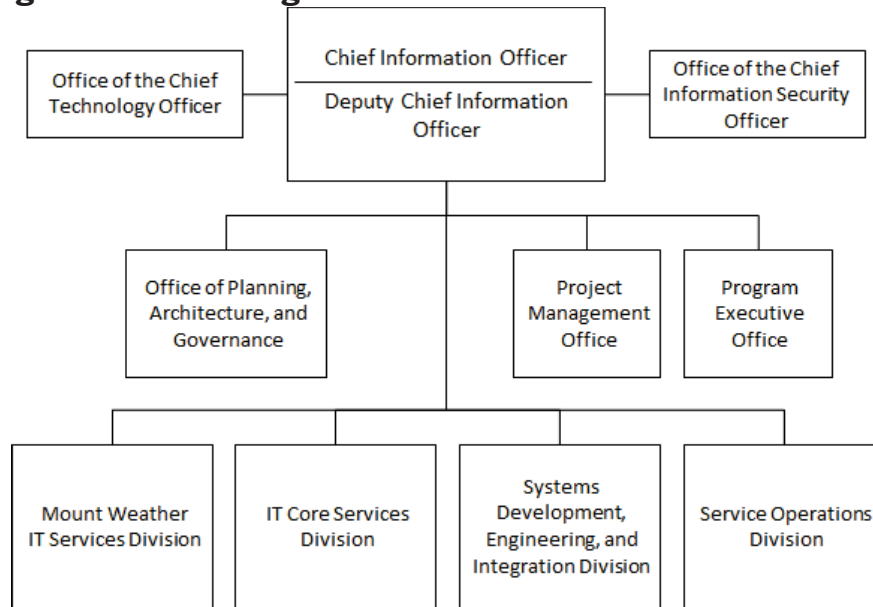
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Mission Support – provides customer-focused business management services and a support infrastructure to enable FEMA's mission success.

The Office of the Chief Information Officer (OCIO) is part of FEMA's Mission Support area. OCIO is responsible for enhancing and maintaining the information technology (IT) infrastructure, developing and enhancing key IT systems, and increasing efficiencies and cooperation across the entire FEMA organization. OCIO partners with FEMA program and regional offices to provide support for systems development, testing, implementation, and operations and maintenance efforts. OCIO employs more than 1,000 staff, including approximately 450 Federal employees and 600 contractors. In FY 2014, FEMA's IT spending was approximately \$450 million. To plan and manage FEMA's critical IT environment, OCIO is organized into nine offices and divisions, as shown in figure 1.

Figure 1. OCIO Organizational Structure as of October 2014



Source: DHS Office of Inspector General (OIG)-generated from FEMA OCIO organization information.

The nine OCIO offices and divisions include:

- Office of the Chief Technology Officer – responsible for leading the technology strategy and direction for a wide variety of mission, business, and enterprise systems, and for providing guidance, advisory services, and investment and change management planning.
- Office of the Chief Information Security Officer – provides cyber security management services to FEMA's emergency management and continuity mission by using the Federal Cyber Security Framework.
- Office of Planning, Architecture, and Governance – provides daily management of the IT Governance Unit and Enterprise Architecture Unit.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Project Management Office – manages the IT Project Management Framework in support of IT policy and procedural compliance.
- Program Executive Office – provides direct support to IT systems and programs requiring direct OCIO oversight.
- Mount Weather IT Services Division – provides specialized support and operations for the entire emergency management community of the Mount Weather Emergency Operations Center.²
- IT Core Services Division – provides the leadership and oversight to establish and direct IT resource management, quality assurance, and customer relationships to foster effective and efficient operations across OCIO and support FEMA missions.
- Systems Development, Engineering, and Integration Division – provides the leadership and oversight to establish and direct the underlying business functions necessary to foster effective and efficient operations throughout OCIO and support missions across the entire FEMA enterprise.
- Service Operations Division – manages disaster systems planning and response, including Joint Field Office support, disaster response team support, mobile systems management and mobile devices, regional coordination, and disaster emergency communications coordination.

OCIO is responsible for enhancing and maintaining IT infrastructure, developing and enhancing key systems to support operating programs, and increasing efficiencies and cooperation across FEMA. FEMA's IT systems include:

Response and Recovery Systems

- National Emergency Management Information System (NEMIS) – a system of hardware, software, telecommunications, and applications that provides a technology base to FEMA and its partners to carry out the emergency management mission. NEMIS was developed to integrate and automate tools to support operations.
- Emergency Management Mission Integration Environment (EMMIE) – a web-based electronic grants system used to manage grants throughout the entire grant life cycle. Using EMMIE, grantees are able to apply for, view the status of, and manage their grants.
- Web-based Emergency Operations Center (WebEOC) – a facility that supports emergency management processes and functions by providing a real-time common operating picture for FEMA headquarters, regions, and Federal, state, local, and tribal strategic partners.

² The mission of the Mount Weather Emergency Operations Center is to manage, operate, and maintain the center in support of FEMA and other Federal departments' and agencies' emergency management programs at all times and under all conditions. The center provides facilities, logistics support, communications, operations centers, and supporting personnel for a wide variety of vital government functions.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Financial Systems

- Web Integrated Financial Management Information System (WebIFMIS) – maintains all FEMA financial data and is the source of financial data for both internal and external financial reporting.
- Enterprise Coordination and Approval Process System (eCAPS) – a web-based application that provides electronic coordination, processing, and approval of mission assignments, which are used for tasking and reimbursing other Federal departments and agencies to provide essential assistance and the requisitions for services and supplies.

Mitigation and Preparedness Systems

- Non-Disaster Grants Management System (ND-Grants) – a web-based system intended to provide FEMA and its stakeholders with a system that supports the grants management lifecycle.
- Mitigation Electronic Grants (eGrants) – a web-based electronic grants system that provides administration and processing of Hazard Mitigation Assistance grants for state and tribal governments.

In a 2011 audit, we identified challenges with FEMA's IT management and infrastructure.³ Specifically, we reported that FEMA had begun a number of necessary modernization efforts; however, OCIO faced challenges in modernizing information technology because it had not yet completed effective IT plans, such as an IT strategy or a baseline enterprise architecture. In addition, program and regional offices continued to develop IT systems independent of OCIO, due in part to decentralized IT budget and acquisition practices. Finally, although FEMA had completed a number of IT infrastructure upgrades and improvements, the agency's critical mission support systems showed little signs of modernization.

³ *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology*, OIG-11-69, April 2011.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Results of Audit

IT Planning Progress and Challenges

Since our 2011 audit, FEMA has developed numerous IT planning documents, including the *FEMA 2013–2016 Technology Management Strategic Plan*, the *FEMA IT Strategic Plan FY 2013–2016*, the *FEMA OCIO's 2013–2014 Annual Plan*, and the *FEMA OCIO Business Transformation Project: Findings and Recommendations*. However, the agency has not effectively coordinated, executed, or followed through on these plans, in part because of the frequent turnover in the CIO position within FEMA. In addition, the need to respond to and address other FEMA priorities identified during reviews of IT programs forced the CIO to reevaluate FEMA's IT modernization approach. During our field work, the CIO was in the process of developing a new IT modernization plan. However, this plan had not been finalized at the end of our field work in March 2015. Without a consistent strategic plan that includes strong progress evaluation reporting, FEMA risks making limited progress in improving IT as needed to support the agency's mission.

Various IT Planning Documents Developed

The *Government Performance and Results Act Modernization Act of 2010* holds Federal agencies responsible for strategic planning to ensure efficient and effective operations and use of resources to achieve mission results.⁴ Additionally, the *Clinger-Cohen Act of 1996*, enacted as part of the National Defense Authorization Act for Fiscal Year 1996, and Office of Management and Budget (OMB) Circular A-130, as revised, instruct agency CIOs to create a strategic plan that demonstrates how information resources will be used to improve the productivity, efficiency, and effectiveness of government programs.⁵ DHS Management Directive 0007.1 requires component CIOs to develop and implement IT strategic plans that clearly define how IT supports the agency's mission and drives investment decisions, guiding the agency toward achieving its goals and priorities.⁶

Since 2011, FEMA has created numerous IT planning documents. Specifically, a technology advisor to the FEMA Administrator created the *FEMA 2013–2016 Technology Management Strategic Plan*. The purpose of this strategic plan was to establish a set of guiding observations about the FEMA operating environment and a course of action for FEMA to develop a new approach to

⁴ Public Law 111–352, January 4, 2011.

⁵ Public Law 104–106, February 10, 1996, and Public Law 104–208, September 30, 1996; OMB Circular A-130, *Management of Federal Information Resources*, Transmittal Memorandum #4, November 28, 2000.

⁶ DHS Management Directive 0007.1, *Information Technology Integration and Management*, March 15, 2007.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

technology management. The plan articulates an agency-wide technology mission statement—“Technology at FEMA exists to empower people first, ideas second, and hardware third through outcome-oriented design, development and management.” The plan consists of four parts:

- Observations – general aspects of FEMA’s operating environment in light of the technology it uses;
- Orientation – how to view this operating environment so that FEMA can accomplish strategic outcomes;
- Decisions – a set of strategic decisions consistent with the FEMA strategic plan initiatives; and
- Actions – nine initial actions to implement this plan.

In addition, in February 2013, the Acting CIO issued the *FEMA IT Strategic Plan FY 2013–2016* to provide guidance for putting the *FEMA 2013–2016 Technology Management Strategic Plan* into action. The *FEMA IT Strategic Plan* aligns with the *DHS IT Strategic Plan for FY 2011–2015* and the *FEMA Strategic Plan FY 2011–2014*. The *FEMA IT Strategic Plan* describes the CIO’s mission, goals, and objectives through FY 2016. Table 1 provides the mission statement and the six goals included in the plan.⁷

Table 1. *FEMA IT Strategic Plan FY 2013–2016* Mission and Goals

FEMA IT Mission:					
Support the FEMA missions through a Whole Community approach, leveraging field-level oriented technology and innovation, in order to achieve positive outcomes for citizens and first responders. This is accomplished by enhancing and maintaining IT infrastructure, developing and enhancing key systems to support operating programs, and through increased efficiencies and cooperation throughout the Whole Community.					
Goal 1	Goal 2	Goal 3	Goal 4	Goal 5	Goal 6
Foster a Whole Community approach to emergency management nationally.	Build the nation’s capacity to stabilize and recover from a catastrophic event.	Build unity of effort among the entire emergency management team through communication, coordination, and collaboration.	Increase FEMA’s own learning through accountability to the Whole Community.	Build, sustain, and improve FEMA’s mission support and workforce capabilities.	Transform the organizational health of the FEMA IT community by developing an exceptional workforce that will function effectively, deliver operational excellence, and grow from within.

Source: DHS OIG-generated from *FEMA IT Strategic Plan FY 2013–2016*.

The *FEMA IT Strategic Plan* contains specific objectives for each goal. For example, one of the three objectives to meet the first goal of fostering a Whole Community approach to emergency management nationally is that the OCIO participate in the FEMA-sponsored, Whole Community technology strategy

⁷ The FEMA strategic plan advances a “Whole Community” approach to the practice of emergency management that emphasizes that it takes all aspects of a community (volunteer, faith, and community-based organizations; the private sector; and the public, including survivors themselves)—not just the government—to effectively prepare for, protect against, respond to, recover from, and mitigate against any disaster.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

initiative, and subsequently map annual updates of the *FEMA IT Strategic Plan* to relevant aspects of the technology strategy developed. The common purpose of the technology strategy initiative is to enhance the nation's preparedness, mitigation, and recovery capabilities.

In April 2013, the Acting CIO also implemented the *FEMA OCIO's 2013–2014 Annual Plan*. The purpose of this OCIO annual plan is to identify specific projects and associated performance metrics that the OCIO could track to assess progress toward the goals and objectives in the *FEMA IT Strategic Plan FY 2013–2016*. The OCIO annual plan includes 11 strategic priority projects as shown in table 2.

Table 2. 11 Strategic Priorities from *FEMA OCIO's 2013–2014 Annual Plan*

Strategic Priority	Description
1. Implement Automation Modernization	Includes 4 projects to modernize FEMA's IT for better performance: 1) expansion of smartphone and tablet use; 2) increased data openness; 3) enhance continuity of operations; and 4) improve system redundancy.
2. IT Governance, Alignment, and Compliance	Implement a standardized, beginning-to-end project review process in accordance with DHS' System Engineering Life Cycle to ensure alignment with FEMA's Enterprise Architecture.
3. Mission Critical System Stabilization	Identify and update hardware and software that are out-of-date. Migrate systems to achieve database consolidation.
4. Managing Systems Sustainment	Implement a process to track the identification, evaluation, development, implementation, and operation of new FEMA mission IT requirements.
5. FEMA's Enterprise Architecture Maturity	Improve FEMA's Enterprise Architecture score and support DHS' mandated reporting requirements.
6. IT Security Plan	Improve the protection of information and information assets while enabling the FEMA mission.
7. Mission Critical Application Enhancements	Improve the usability, sustainability, and compatibility of FEMA's aging systems.
8. A New Joint Field Office Solution	Improve IT service capabilities and delivery to FEMA's Joint Field Office facilities.
9. eWorkplace Transformation	Provide IT support to the FEMA Administrator's Workplace Transformation Initiative to allow FEMA employees to work outside of a traditional workplace environment.
10. OCIO Business Transformation	Conduct an evaluation of baseline OCIO capabilities and provide recommendations to improve OCIO service delivery to our customers by institutionalizing IT best practices.
11. Multi-Level Governance	Implement an enterprise-wide, multi-layered, collaborative governance process.

Source: DHS OIG-generated from *FEMA OCIO's 2013–2014 Annual Plan*.

For each of the 11 strategic priorities, the OCIO annual plan identifies criteria for measuring success, as well as specific tasks with due dates and assignments of responsibility. The plan indicates that OCIO will conduct monthly progress reviews and create evaluation reports to compare actual performance against defined metrics to facilitate continuous process improvement.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Finally, in addition to these plans, the Acting CIO issued *FEMA OCIO Business Transformation Project: Findings and Recommendations* in May 2013. The purpose of this report was to present the findings and recommendations from a major internal evaluation of capability and performance gaps within OCIO. The report provides the foundation for a major transformation of OCIO, which was included in the *FEMA OCIO's 2013–2014 Annual Plan* as strategic priority number 10. Table 3 lists the report's eight recommendations.

Table 3. Recommendations from *FEMA OCIO Business Transformation Project: Findings and Recommendations*

Recommendation	Overview
1. Implement a more holistic approach to OCIO communications.	OCIO leadership and staff identified the need for improved communications as a major priority within the FEMA OCIO.
2. Actively promote the cultural change.	The culture within the OCIO has evolved into one of react and respond. In order to become a best practice-based, customer-focused, and outcome-oriented organization, the culture needs to evolve to be more forward thinking and strategic.
3. Reorganize to improve customer focus and service.	The OCIO should reorganize to improve its ability to perform at a best-practice level and to overcome operational issues identified within the organization.
4. Adopt a strategic approach to workforce management.	The OCIO needs to adopt a strategic approach to how it acquires, develops, deploys, motivates, evaluates, and rewards its people.
5. Improve corporate IT planning, management, and governance.	The OCIO has yet to define and implement a mix of enterprise-level IT planning, management, and governance activities that are reflective of how best practice-based organizations plan and manage their activities.
6. Conduct core IT life cycle and business management process analyses and improvement efforts.	The OCIO has not fully developed core IT life cycle and business management processes or identified root causes for lack of adherence to existing processes. The OCIO must develop and implement an IT life cycle and business management process improvement plan.
7. Empower the CIO to implement IT Transformation.	FEMA should define and begin implementing a process for moving all IT budget control and spending under the CIO. This transition to full CIO control of IT spending should be done in a manner that is well-planned and reasonably paced to ensure that OCIO has the capacity to manage the increase in IT management and investment responsibility. Full empowerment includes elevating the FEMA OCIO to the same level as the Chief Financial Officer position and directly reporting to the Administrator.
8. Establish a Transformation Management Team.	For transformation to be successful, it must be managed like any other project or program. As such, it should have clear objectives and scope, a project leader and team, appropriate resources, a schedule and work plan, and measurable results.

Source: *FEMA OCIO Business Transformation Project: Findings and Recommendations*, May 2013.

While the business transformation report contains a high-level action plan for implementing these recommendations, it also identifies the need for OCIO to create a more detailed implementation plan going forward.

Coordination, Execution, and Follow-Through on Various Plans Needs Improvement

Although FEMA has developed numerous IT planning documents, the agency has not effectively coordinated, executed, or followed through on these plans.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Table 4 contains our evaluation of these plans. Without coherent planning that includes strong implementation progress reporting, FEMA puts at risk its progress in improving IT as needed to support the FEMA mission.

Table 4. OIG Evaluation of Various IT Planning Documents

Planning Document Title	OIG Evaluation
<i>FEMA 2013-2016 Technology Management Strategic Plan</i>	<ul style="list-style-type: none">• Does not clearly articulate why FEMA needed a plan developed outside of the OCIO, or how it interrelates with other OCIO plans in place at the time.• Does not contain specific targets or metrics to evaluate progress.
<i>FEMA IT Strategic Plan FY 2013-2016</i>	<ul style="list-style-type: none">• The OCIO has not updated this plan since it was issued in February 2013. The plan states that it will be updated on an annual basis to maintain currency with FEMA, DHS, and Federal government guidance and strategies, as well as changes to technology and best IT and business practices.• This plan is intended to align with the FEMA strategic plan and the DHS IT strategic plan, which have both been updated since February 2013.
<i>FEMA OCIO's 2013-2014 Annual Plan</i>	<ul style="list-style-type: none">• The OCIO has not issued an annual plan since the initial one dated April 2013.• The OCIO has not conducted monthly progress reviews, as required by the plan. The last OCIO meeting to discuss the progress made in meeting the goals and objectives was held in August 2013.• The OCIO has not prepared evaluation reports to compare actual performance against defined metrics, as required by the plan.
<i>FEMA Office of the Chief Information Officer Business Transformation Project: Findings and Recommendations</i>	<ul style="list-style-type: none">• The OCIO has been inconsistent in executing these recommendations, and has not issued a detailed implementation plan.<ul style="list-style-type: none">○ For example, recommendation 3 to reorganize the OCIO was being completed during our fieldwork.○ However, recommendation 7 to empower the CIO by moving all IT budget control and spending under the CIO and elevating the OCIO to report directly to the FEMA administrator was not being pursued. Instead, the current CIO has adopted the approach that the OCIO does not have to control the FEMA IT enterprise to influence it.

Source: DHS OIG-generated based on analysis of IT planning documents.

Frequent CIO Turnover and New Priorities Contribute to Ineffective Planning

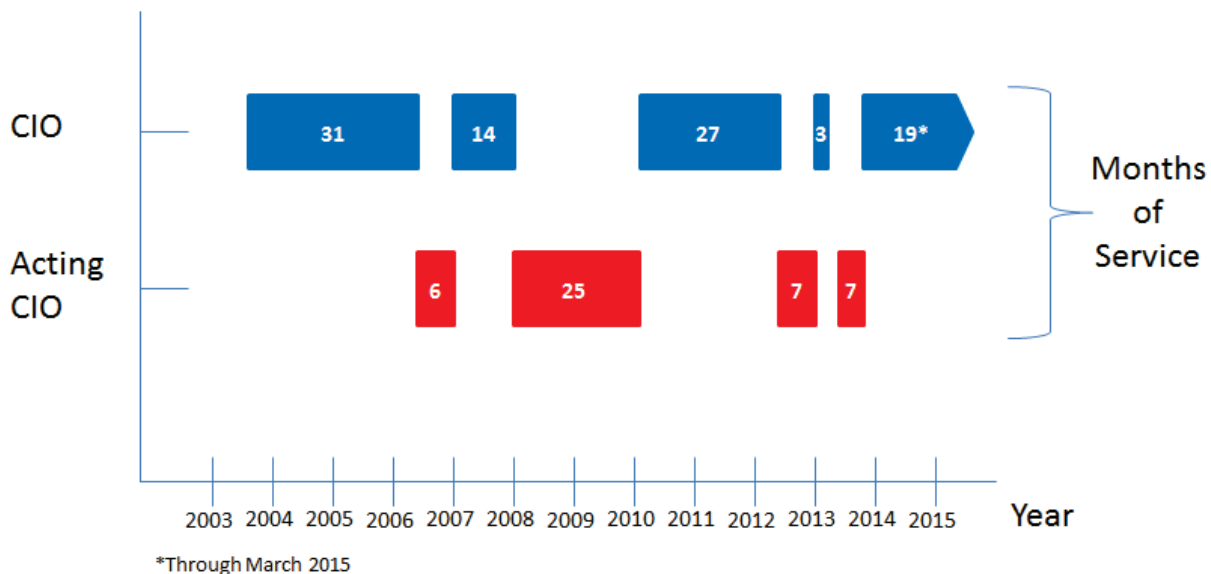
FEMA has not effectively coordinated, executed, or followed through on its plans, in part because of the frequent turnover in the CIO position within the agency. FEMA has had six different individuals, either appointed or acting, serving in the CIO position over the past 10 years. For this time period, the average tenure of the FEMA CIO has been 15 months. In the last 3 years alone, FEMA had four different individuals in the CIO position. Figure 2 shows the numerous transitions from appointed to acting leadership within OCIO since 2003.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 2. Transitions from Appointed to Acting CIOs Since 2003



Source: DHS OIG-generated.

The current CIO, who assumed responsibility in September 2013, encountered new Federal priorities that diverted his IT focus and attention. Specifically, the results of a CyberStat review conducted by the National Security Council, OMB, and DHS Headquarters personnel identified significant deficiencies at FEMA that could cause harm to the Department's security program if not corrected timely. CyberStat reviews are face-to-face, evidence-based meetings to evaluate agencies' cybersecurity performance and identify mechanisms to ensure that agencies are on track to achieve the President's cybersecurity performance goals. As a result, the FEMA Administrator directed the CIO to conduct onsite information cybersecurity and business process resilience reviews. These reviews, which were conducted between January and September 2014, covered all 10 FEMA Regions and all headquarters programs and offices and became the focus of the new CIO's approach to understanding and improving FEMA's IT environment.

In addition, in September 2014, the Deputy Administrator issued a 90-Day Plan to drive the agency's progress in achieving the Administrator's priorities. This 90-Day Plan required the CIO to take specific actions to stabilize and drive the modernization of FEMA mission and business systems. Among other requirements, it called for the CIO to develop yet another plan—a comprehensive *FEMA Mission and Business Systems Modernization Plan* to:

1. define the Agency's IT modernization approach;
2. prioritize IT investments against FEMA's strategic priorities based on input from FEMA components;



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

3. establish clear targets and metrics for evaluating success in achieving targets; and
4. establish an IT investment strategy for FY 2016–2020.

To address this requirement, the CIO drafted and was finalizing a new *FEMA IT Modernization Plan* during our field work. The CIO's approach to modernizing FEMA's IT environment to meet user and customer needs consisted of three phases to be completed over the next 5 years:

1. stabilization of FEMA's IT environment by addressing immediate, high-priority IT security risks;
2. optimization of FEMA's IT environment through better governance and reduced duplication; and
3. transformation of FEMA's IT environment into a modern suite of mission applications and systems that better supports the needs of survivors, first-responders, and community partners.

Until a finalized plan with rigorous performance metrics is in place, the CIO will face challenges in communicating and enforcing a common IT strategic direction across all of FEMA.

Recommendations

We recommend that the FEMA CIO:

Recommendation 1: Finalize necessary IT planning documents that reflect the current IT strategy of the organization and IT modernization initiatives.

Recommendation 2: Execute the planning documents, using the milestones and metrics included in them to evaluate FEMA's long-term progress in improving its IT management and operations.

OIG Analysis of FEMA Comments

We obtained written comments on a draft of this report from the Acting Associate Administrator for the Office of Policy and Program Analysis at FEMA. We have included a copy of the comments in their entirety in appendix B.

In the comments, the Acting Associate Administrator concurred with our recommendations and provided details on the current actions to address specific findings and recommendations in the report. We have reviewed management's comments and provided an evaluation of the issues outlined in the comments that follow.

In response to recommendation 1, the Acting Associate Administrator concurred and stated that the FEMA CIO is initiating FEMA-wide IT



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

modernization efforts. FEMA plans to finalize the *FEMA IT Modernization Plan* by the first quarter of FY 2016. The plan is intended to transition FEMA from its current business and technology environment to its target environment over a 5-year period. FEMA's IT Governance Board (ITGB), and its subordinate Integrated Project Teams, are responsible for governing the modernization plan's development. We recognize FEMA's efforts to complete the *FEMA IT Modernization Plan* as a positive step toward addressing recommendation 1 and look forward to reviewing the plan once it is completed. This recommendation is open and resolved.

Responding to recommendation 2, the Acting Associate Administrator concurred and stated that FEMA will evaluate the long-term progress in improving its IT management and operations by continuing to implement the strategic roadmap to IT modernization. FEMA is focusing on the consolidation, modernization, and integration of key business systems in five areas, including Financial Systems, Grants Systems and Human Resources Systems. Together 5 key business areas encompass nearly 100 systems that are inefficiently tied together in such a way that inhibits FEMA's ability to achieve its strategy. The target architecture is intended to simplify systems within these business areas. Other FEMA transformational efforts grounded in modernization include cyber security, infrastructure, and Regional IT. We look forward to learning more about continued progress and improvements in the future. This recommendation is open and resolved.

Effective IT Governance Has Not Yet Been Fully Established

FEMA's efforts to implement agency-wide IT governance have not been fully effective. FEMA instituted the ITGB in February 2012; however, the board's functioning proved ineffective and it eventually stopped holding meetings. In September 2014, FEMA established a new ITGB, but at the time of our audit field work that new board's charter was still being finalized and was not yet fully effective. FEMA has struggled to implement effective agency-wide IT governance, in part because the CIO has not had sufficient control and budget authority to effectively lead the agency's decentralized IT environment. Without effective agency-wide IT governance, FEMA's IT environment has evolved over time to become overly complex, including a large inventory of systems, which are difficult to secure and costly to maintain.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

IT Governance Boards

According to Federal guidance, agencies are required to implement IT governance structures to ensure effective management of IT resources.⁸ In addition, OMB has recently issued guidance as part of a Federal IT management reform plan aimed at increasing CIO authority, including in areas such as IT governance.⁹

In February 2012, FEMA issued a directive that defined the authorities of the CIO and instituted, among other things, the ITGB with responsibility for agency-wide IT governance.¹⁰ The purpose of the ITGB was to create a decision forum for the CIO to engage leadership across the FEMA enterprise to ensure that IT enabled the agency's mission and that IT resources were properly allocated. The CIO issued a charter that detailed the composition, authorities, responsibilities, and duties of the ITGB. The charter identified 12 voting members, including members from among FEMA's program areas and regions, with the CIO and Deputy Administrator of FEMA serving as co-chairs. The board's primary responsibilities included assisting the CIO in setting the IT strategic direction; evaluating, approving, and monitoring all agency IT investments; and validating IT requirements.

The ITGB chartered in 2012 was not effective. In early 2013, OCIO conducted an internal evaluation of how well 22 IT management functions and processes were being performed and assigned a rating of red (poor or very poor), yellow (average), or green (good or excellent) to each function or process based on the results of its evaluation. IT governance received a rating of red, in part because the ITGB did not meet on a regular basis. Specifically, the board had convened only six times and held its last meeting in May 2012.

In addition, the board struggled to make decisions on FEMA-wide IT initiatives. For example, the *Consolidated Appropriations Act, 2012*, allocated \$13.662 million for FEMA to modernize IT systems.¹¹ One of the main initiatives undertaken by the ITGB was to decide which projects should receive this funding. However, the process the board implemented to solicit, evaluate, and select candidate IT projects was unsuccessful. The board did not use the results obtained from this process because members did not concur with the scoring results. Instead, the board moved forward with a plan to allocate the funding to three projects that were put forward without a formal process for evaluating IT priorities FEMA-wide.

⁸ Public Law 104-106, February 10, 1996, and Public Law 104-208, September 30, 1996; OMB Circular A-130, November 28, 2000.

⁹ OMB M-11-29, *Chief Information Officer Authorities*, August 8, 2011; OMB M-13-09, *FY 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, March 27, 2013.

¹⁰ FEMA Directive 140-2, February 10, 2012.

¹¹ Public Law 112-74.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In September 2014, the CIO reestablished the ITGB as called for in the Deputy Administrator's 90-Day Plan. The draft charter for the new ITGB contained a number of differences from the prior ITGB, intended to improve its effectiveness. For example, the new charter expanded ITGB membership to include 18 members, 3 of which were Regional Administrators. The charter established a goal that 25 percent of board membership would be composed of managers and supervisors from headquarters and field offices who have direct day-to-day experience with IT systems and could best represent system users' needs. The new charter also strengthened the role of the board's co-chairs in the decision process giving them, along with the FEMA Chief of Staff, decision authority if the board could not reach consensus. The new ITGB has met regularly since its establishment in September 2014. Table 5 provides a comparison of the prior ITGB chartered in 2012 and the newly reestablished ITGB.

Table 5. Comparison of Prior and New ITGBs

Prior ITGB (Instituted in 2012)	New ITGB (Reestablished in 2014)
Representation	
<ul style="list-style-type: none">• 12 members• 2 Regional Administrators	<ul style="list-style-type: none">• 18 members• 3 Regional Administrators• Goal to have 25% membership be headquarters and field staff with direct day-to-day experience with IT systems
Decision Process	
<ul style="list-style-type: none">• If consensus cannot be reached, disagreement is documented and referred to a senior decision authority	<ul style="list-style-type: none">• If consensus cannot be reached, Co-Chairs and FEMA Chief of Staff have decision authority
Meeting	
<ul style="list-style-type: none">• Met 6 times over 5 months• Last meeting held in May 2012	<ul style="list-style-type: none">• Met 11 times in 8 months

Source: DHS OIG analysis of ITGB charters and meeting minutes.

These changes to the membership, decision process, and frequency of meetings have the potential to make the reestablished ITGB more effective than the original board. However, the new board was not yet fully established at the time of our field work, which ended in March 2015. The charter for the board was still in draft and not yet finalized. In addition, many of the processes and tools needed to allow the board to address inefficiencies, such as redundant systems in the current IT environment, as well as evaluate new IT investment decisions, were still being developed. For example, OCIO was still finalizing the blueprint for FEMA's target IT environment as needed to analyze and prioritize new IT investments.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Given the inconsistent agency-wide IT governance, FEMA's IT environment has evolved over time to become overly complex. Specifically, in 2014, OCIO undertook a year-long effort to complete FEMA's first comprehensive inventory of IT systems across all headquarters components and FEMA's 10 regions. The inventory identified 200 systems, which OCIO considered twice as many as an organization the size of FEMA should have. This complex IT environment is difficult to secure. Our FY 2014 *Federal Information Security Management Act* report, along with National Security Council and OMB reviews, have identified IT security weaknesses and vulnerabilities that limit FEMA's ability to ensure the confidentiality, integrity, and availability of critical data.¹² For example, FEMA had five "Top Secret" systems that had been operating without the proper authority; some authorities to operate had been expired since August 2013.

The existing complex IT environment is also costly to maintain. FEMA has numerous obsolete systems, such as the 20-year-old financial system, WebIFMIS, that are difficult and costly to maintain and need replacement. The high cost of maintaining the existing system environment limits funding for system replacement or addressing new system needs. Until agency-wide IT governance is fully established with adequate CIO authority, FEMA will continue to face challenges improving the efficiency of its current IT environment, and efforts to transform and modernize FEMA's IT will remain at risk.

FEMA CIO Does Not Have Agency-wide IT Authority

FEMA has struggled to implement effective agency-wide IT governance, in part, because the CIO has not had sufficient authority to effectively lead the agency's decentralized IT environment. Specifically, the CIO does not directly control most IT funding within FEMA. In our 2011 report, we found that the OCIO budget accounted for only approximately one-third of the agency's IT spending, with the FEMA program offices accounting for the remaining two thirds. This decentralized IT funding approach has not changed significantly since our last report. The OCIO's FY 2014 IT spending was approximately \$170 million, which accounted for approximately 38 percent of FEMA's agency-wide IT spending total of approximately \$450 million, as shown in figure 3.

¹² *Evaluation of DHS' Information Security Program for Fiscal Year 2014*, OIG-15-16, December 12, 2014.

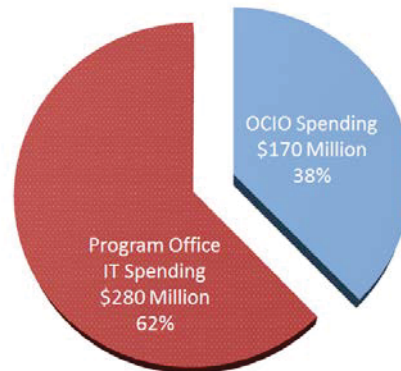


OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 3. FEMA FY 2014 IT Spending

FEMA IT Spending for FY 2014
Approximately \$450 Million



Source: DHS OIG-generated from FEMA data.

In addition, the CIO does not control all FEMA IT personnel. As of September 2014, 177 personnel worked in IT functions within FEMA components that were not part of OCIO. Table 6 shows the FEMA components that had IT personnel independent from the CIO.

Table 6. FEMA IT Personnel

Location of IT Staff	Number
IT Personnel Within the OCIO	454
IT Personnel Outside of the OCIO	
• FEMA's 10 Regions	106
• Office of Response and Recovery	44
• Protection and National Preparedness	17
• Other	10
Total:	177

Source: DHS OIG-generated from FEMA data.

Although FEMA has implemented policies to provide the CIO with more agency-wide control, such policies have not been fully effective. For example, in February 2012 FEMA issued Directive 140-2: *FEMA Information Technology Integration and Management*. The purpose of this directive was to define the CIO authorities to lead the agency's IT environment. However, it was this directive that instituted the original ITGB that proved ineffective and ultimately stopped meeting. The 2012 directive also implemented an agency-wide IT investment review process, but an internal evaluation conducted by OCIO approximately one year later found that the directive had not given the CIO adequate oversight of IT spending—a significant amount of funds were still being spent on IT investments outside of the CIO's control. In September 2014,



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

the FEMA Deputy Administrator called for a revision to the IT investment review process, which was in draft during our audit field work.

Further, the CIO's organizational position within FEMA may hinder his ability to adequately implement and enforce agency-wide IT policies. Specifically, Federal law states that agency CIOs shall report directly to the head of the agency.¹³ This requirement does not specifically apply to FEMA, which is considered a component of a larger agency, DHS. However, the CIO reports to the Associate Administrator for Mission Support within FEMA. In contrast, FEMA's Regional Administrators and Associate Administrators for headquarters components report directly to the FEMA Administrator. Given this, the CIO has struggled to exert adequate influence on IT spending and fully enforce agency-wide IT management practices. For the CIO to implement an effective IT governance structure in collaboration with component leadership, the CIO could benefit from equal stature with them organizationally.

Recommendations

We recommend that the FEMA CIO:

Recommendation 3: Finalize the ITGB charter and expand the capacity of the board to make the board the IT decision-making authority for the agency.

OIG Analysis of FEMA Comments

In response to recommendation 3, the Acting Associate Administrator concurred and reported that the ITGB members signed the Charter on May 7, 2015, officially establishing the board as the IT decision-making authority for FEMA. FEMA has provided the audit team with a copy of the finalized ITGB Charter. Additionally, the Acting Associate Administrator provided a list of ITGB board members who come from different areas of the agency, and stated that these board members expand the ITGB's capacity to make FEMA-wide decisions. FEMA has taken adequate steps to address this recommendation. This recommendation is closed.

IT Systems Do Not Fully Support Mission Needs

FEMA IT systems do not provide fully effective support to the agency's mission needs. Specifically, in the complex, decentralized IT environment resulting from a lack of agency-wide IT governance, FEMA personnel have to manually enter information into numerous IT systems that are not sufficiently integrated. Some FEMA systems also do not have needed data search and reporting tools, and FEMA personnel must obtain and consolidate information from multiple screens or implement manual workarounds. FEMA's systems are not integrated

¹³ Public Law 104-13, *Paperwork Reduction Act of 1995*, May 22, 1995.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

and do not fully provide needed capabilities because, in part, they have been developed, patched, and interconnected in an ad hoc manner. As a result of system limitations, end users engage in inefficient, time-consuming business practices, creating their own tools such as spreadsheets and databases. Because of such inefficient work practices, FEMA faces increased risk that disaster assistance and grants could be delayed and duplication of benefits could occur.

IT Systems Are Not Sufficiently Integrated

According to the *Clinger-Cohen Act of 1996*, the CIO is responsible for developing, maintaining, and facilitating the implementation of a sound and integrated IT environment.¹⁴ The *Paperwork Reduction Act of 1995* requires agencies to acquire, use, and manage IT to improve mission performance.¹⁵ Also at the Department level, DHS Management Directive 0007.1 requires component CIOs to deliver mission IT services in a timely manner and in direct support of the component's mission, goals, objectives, and programs.¹⁶

FEMA has numerous IT systems that are not sufficiently integrated to effectively support the needs of agency personnel. For example, FEMA has nine different systems that support the agency's grant programs. Each of these systems was developed independently to support a specific type of grant. Table 7 identifies the four major grant systems that we assessed during this audit and their specific purposes.

¹⁴ Public Law 104-106, February 10, 1996.

¹⁵ Public Law 104-13, May 22, 1995.

¹⁶ DHS Management Directive 0007.1, March 15, 2007.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Table 7. Major Grant Systems

System	Type of Grant	Description
Disaster Grants		
NEMIS	Individual Assistance Grants	Assistance to individuals to aid in the recovery from disasters.
EMMIE	Public Assistance Grants	Assistance to state, tribal, and local governments, and certain types of private nonprofit organizations so that communities can quickly respond to and recover from disasters.
Non-Disaster Grants		
eGrants	Mitigation Grants	Assistance to reduce loss of life and property by lessening the impact of disasters.
ND-Grants	Preparedness Grants	Assistance to enhance the capacity of state and local emergency responders to prepare for various man-made threats.

Source: DHS OIG-generated from FEMA data.

These systems do not enable grant managers to monitor FEMA activity across grant programs. For example, grant managers cannot easily determine the grant activity for a particular state across the various grant programs. Grant managers have to access each of the systems individually, search for open grants to a state, and compile the results. One region had created its own tool for tracking information across FEMA's various grant systems. Personnel said that this tool allows the region to track grant information regardless of the grant system housing the grant. The numerous unintegrated grant systems also create complexity for grant recipients, such as states, who have to access multiple systems to process grant awards and request payment. One grant manager said that this leads to confusion, wasted time, and frequent errors.

Further, FEMA grant systems are not sufficiently integrated with the agency's main financial system, WebIFMIS. FEMA personnel must manually enter information from the grant system into WebIFMIS at certain stages in the grant process. For example, the mitigation grant system, eGrants, interfaces with WebIFMIS for grant awards. However, FEMA personnel must manually enter changes to the grant period of performance—the time period during which the grantee is expected to complete the grant activities—separately in both systems. Similarly, the preparedness grant system, ND-Grants, does not fully interface with WebIFMIS. Personnel must manually enter information to complete and close out a grant in both ND-Grants and WebIFMIS.

As a result of grant systems not being integrated, staff's ability to detect grant duplication is impeded. According to regional staff, if a state were to suffer multiple disasters, one person could apply for assistance for each of the



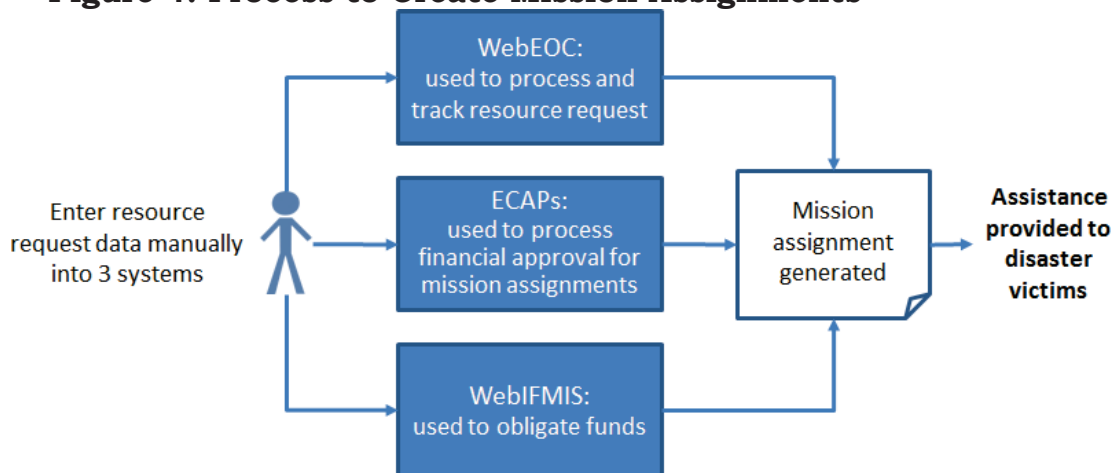
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

different disasters and not be identified. Further, the inability of enterprise systems to accurately transmit grant information between certain systems can result in grantees receiving incorrect notices that they are not in compliance with grant requirements, which has resulted in delays in making grant funds available. When there is a delay in the availability of grant funds, FEMA's ability to achieve its strategic objectives may be hampered.

In addition to the grant systems, FEMA's primary watch and response collaboration system, WebEOC, is not sufficiently integrated with key agency systems. When state or local governments are overwhelmed during a major disaster, FEMA uses mission assignments to request immediate short-term emergency response assistance. FEMA personnel enter information into WebEOC, which processes and tracks the mission assignment requests. Personnel also must manually enter the same information into eCAPS, the financial approval system used to process mission assignments, and WebIFMIS. Figure 4 shows the manual data entry required for the mission assignment process.

Figure 4: Process to Create Mission Assignments



Source: DHS OIG-generated from FEMA data.

Further, the FEMA WebEOC is not integrated with the WebEOC used by state emergency operation centers. FEMA regions rely on an inefficient manual process to update the FEMA WebEOC with information from the state centers about ongoing disasters. Specifically, a region has to send FEMA staff to a state emergency operation center to review the state's information. If a state's request for assistance is submitted in the state system, a FEMA staff member must print it out and manually enter the same data into the FEMA WebEOC. This process can cause delays in providing disaster assistance. For example, during an exercise in one state, FEMA staff had to manually transfer 18 state requests from the state system into the FEMA system before FEMA could process the requests. According to FEMA staff, this caused a delay of between



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

2 to 6 hours, which can be critical in emergency management and response, which involves saving lives and preventing property damage.

IT Systems Do Not Provide Needed Reporting Capabilities

Some FEMA systems do not have effective data search or reporting capabilities. Specifically, major systems, such as NEMIS and EMMIE, cannot easily provide needed information. For example, FEMA personnel cannot simply retrieve from NEMIS a standard report that contains a grant applicant's entire record. Instead, grant personnel must access numerous different screens in NEMIS and compile the results. Similarly, reports in EMMIE can only be prepared for one disaster at a time. To obtain information across several disasters, personnel must access and retrieve a report for each individual disaster and manually combine the data into one report. In addition, one grant specialist said that none of FEMA's non-disaster grants systems were able to generate reports listing open, closed, or expired grants collectively.

To address this gap in reporting capabilities, FEMA implemented the Enterprise Data Warehouse tool to provide improved searches and reports on data in the agency's grant systems. The Enterprise Data Warehouse enables personnel to more easily conduct searches and obtain reports across systems, such as EMMIE and NEMIS, as well as across disasters. However, field personnel said that the information obtained from the Enterprise Data Warehouse is not always accurate. For example, one grant specialist conducted a search for open disasters in the region. The results of the search included disasters that had been closed for years, as well as disasters from outside that region. Another grant specialist identified properties that should have been ineligible for mitigation grants that showed up as eligible in Enterprise Data Warehouse reports.

Systems reporting challenges have resulted in personnel engaging in inefficient, time-consuming business practices on a daily basis. Field personnel also engage in manual workarounds to complete routine tasks. For example, one region had created 30 Excel spreadsheets to have the information needed to report on disaster spending by states in response to a congressional request. In addition, field personnel created their own tools, such as spreadsheets and databases, to fill the gaps from enterprise system limitations. In addition to being inefficient, locally developed tools can create security risks if they contain sensitive information.

Systems Development Approach Has Not Been Effective

FEMA's systems are not integrated and do not fully provide needed capabilities because, in part, they have been developed, patched, and interconnected in an ad hoc manner. Historically, FEMA has not had a comprehensive requirements



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

management process in place agency wide. Individual components within FEMA developed systems without adequate business cases or adherence to systems development life cycle guidance. Consequently, systems were developed in silos without attention to overlap, duplication, or the need for integration with other systems. In addition, headquarters components within FEMA developed systems to meet headquarters needs, without adequate inclusion of the requirements of field personnel from the agency's regional offices. The current CIO has acknowledged this challenge and has made it a priority to implement a comprehensive requirements management process and improve adherence to systems engineering life cycle guidance. As a first step, the CIO has focused on completing business cases for the systems currently in FEMA's inventory.

Recommendations

We recommend that the FEMA CIO:

Recommendation 4: Implement a plan of action and milestones to address the integration and reporting limitations of existing systems.

Recommendation 5: Implement and enforce a standardized, agency-wide process that sufficiently defines and prioritizes the acquisition, development, operation, and maintenance requirements for all systems.

OIG Analysis of FEMA Comments

In response to recommendation 4, the Acting Associate Administrator concurred and stated that the *FEMA IT Modernization Plan*, which FEMA plans to finalize by the first quarter of FY 2016, outlines initiatives that the ITGB has identified as necessary for modernization over the next 5 years. Each initiative is aligned with IT systems from the FEMA systems inventory; an Integrated Project Team was formed to complete each initiative. These Integrated Project Teams are chartered to develop and execute a detailed implementation Plan of Action and Milestones to address integration and reporting limitations of existing systems. We recognize this action as a positive step and look forward to learning more about continued progress in the future. This recommendation is open and resolved.

Responding to recommendation 5, the Acting Associate Administrator concurred and stated that FEMA will implement and enforce a standardized, agency-wide process that sufficiently defines and prioritizes the acquisition, development, operation, and maintenance requirements for all systems by exercising authorities through the ITGB. These authorities include approving all IT budget and investment requests, certifying that IT investments are adequately implementing incremental development, and reviewing and



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

approving any contract for IT that is considered a major development. We look forward to learning more about continued progress and improvements in the future. This recommendation is open and resolved.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

In a 2011 audit, we identified challenges in FEMA's IT management and infrastructure. As part of our ongoing responsibilities to assess the efficiency, effectiveness, and economy of the departmental programs and operations, we conducted a follow-up audit to determine whether FEMA's IT management approach addresses planning, governance, and management of technology to support its mission.

We researched and reviewed Federal laws, Department management directives, and agency directives, plans, and strategies related to IT systems, management, and governance. We obtained published reports, documents, testimony, and news articles regarding FEMA's management and use of IT. Additionally, we reviewed recent Government Accountability Office (GAO) and DHS OIG reports to identify prior findings and recommendations. We used this information to establish a data collection approach that consisted of focused information-gathering meetings, documentation analysis, site visits, and system demonstrations to accomplish our audit objectives.

We held meetings and participated in teleconferences with FEMA staff at headquarters and regional offices to learn about FEMA IT functions, processes, and capabilities. At headquarters, we met with the Associate Administrator for Mission Support and FEMA OCIO officials including the CIO, Deputy CIO, Chief Technology Officer, the Chief of Staff, division directors, and other OCIO officials to discuss their roles and responsibilities related to FEMA IT management. We met with division directors and IT officials from the Mount Weather IT Services Division and the OCIO's Service Operations Division in Winchester, Virginia.

We visited FEMA's Region IV in Atlanta, Georgia; Region VI in Denton, Texas; Region IX in Oakland, California; and Region X in Bothell, Washington. During our regional office visits, we met with executive staff, IT officials, Watch Section analysts, grants management staff, and other officials and end users from various offices including Protection and National Preparedness, Response and Recovery, Federal Insurance and Mitigation, and Mission Support to understand user requirements and system use in the field. We discussed FEMA's IT environment, local IT development practices, user involvement, and communication with headquarters. We collected supporting documents about the FEMA IT environment, IT management functions, system challenges, and improvement initiatives.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We conducted this performance audit between November 2014 and March 2015 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

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



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
FEMA Comments to the Draft Report


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



FEMA

OCT 28 2015

MEMORANDUM FOR: Sondra McCauley
Assistant Inspector General for IT Audits
Office of Inspector General

FROM: David Bibo 
Associate Administrator (Acting)
Office of Policy and Program Analysis

SUBJECT: FEMA Management's Response to OIG Draft Report,
"FEMA Faces Challenges in Managing Information
Technology"
(Project number 14-128-IT-FEMA)

Thank you for the opportunity to review and comment on the attached draft report. The Federal Emergency Management Agency (FEMA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

FEMA is maturing its management of information technology (IT) processes by implementing an integrated governance approach. This approach integrates best practices from strategic planning, enterprise architecture, portfolio management, Capital Planning Investment Control, Information Technology Governance Board (ITGB), Project Management Office (PMO), and cyber security with the driving forces of external laws and guidance to enable FEMA and Department-level results. The ITGB plays the key role in FEMA's implementation of the Federal Information Technology Acquisition Reform Act (FITARA), enacted December 19, 2014, and related IT management best practices. The ITGB has the authority to:

- Enhance transparency and improve risk management across FEMA's IT investment portfolio;
- Review and select IT Investments for the FEMA's IT portfolio at least annually;
- Recommend to the IT Investments Business Owner's the termination or retirement of an IT Investment from the FEMA's IT portfolio;
- Direct corrective actions or changes in the management and operation of an IT Investment within the organization;
- Approve or disapprove the initial and any subsequent changes to the IT Investment's performance measurement baseline; and
- Recommend and present to the executive-level, business decision-making authority the list of IT Investments proposed for funding.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Given this report, FEMA will take corrective measures to address the recommendations.

The original draft report contained six recommendations with which FEMA concurred with five of the six recommendations. However, during the exit conference the OIG indicated it plans to remove the non-concur recommendation from the final report. Specifically, the remaining recommendations from the OIG are as follows:

Recommendation 1: Finalize necessary IT planning documents that reflect the current IT strategy of the organization and IT modernization initiatives.

Response: Concur. FEMA CIO is already initiating FEMA-wide modernization efforts. FEMA will finalize the resource loaded “IT Modernization Plan” by the first quarter of FY16. The primary goal of IT modernization is to move FEMA towards the unity of effort needed to implement an integrated governance approach over a five-year period from FEMA’s current business and technology environments to its target environments. The ITGB, and its subordinate Integrated Project Teams, are responsible for governing the plan’s development and use (i.e., directing, overseeing, and making decisions about the plan’s content and implementation).

Estimated Completion Date (ECD): December 31, 2015.

Recommendation 2: Execute the planning documents, using milestones and metrics included in them, to evaluate FEMA’s long-term progress in improving its IT management and operations.

Response: Concur. FEMA will evaluate the long-term progress in improving its IT management and operations by continuing to implement the strategic roadmap to IT modernization. This ongoing effort focuses on the consolidation, modernization, and integration of key business systems in five areas: Financial Systems, Grants Systems, HR Systems, Geospatial Information Systems & Analytics, and SharePoint and Collaboration. These five areas encompass nearly 100 systems currently tied together by a “spaghetti network” of data bases, systems interfaces, and software that inhibit FEMA’s ability to achieve its strategy. The architecture work necessary to simplify the existing spaghetti information network in a way that upholds the common enterprise has led to the creation of FEMA’s Target Architecture. Other transformation efforts grounded in FEMA’s strategic roadmap for IT modernization include:

- Addressing system cyber security and IT resiliency gaps identified during the Review through investments in Plans of Action and Milestones and Enterprise enhancements;
- Improving FEMA’s Infrastructure by moving to Cloud-provided Email as a Service and upgrading FEMA’s Enterprise Voice Network;



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Transforming FEMA Regional IT and Business capabilities by improving how Enterprise-wide IT capabilities are created and deployed; and,
- Reducing FEMA's IT operations and maintenance spend through review of Mission Essential Systems and pursuing opportunities for consolidation of Region IT capabilities.

ECD: March 31, 2016

Recommendation 3: Finalize the ITGB Charter and expand the capacity of the board to make the board the IT decision making authority for the agency.

Response: Concur. The ITGB members signed the Charter on May 7, 2015 to officially establish the board as the IT decision-making authority for the agency. The ITGB is co-chaired by the FEMA Deputy Administrator and FEMA CIO and is comprised of the following members to expand its capacity to make FEMA-wide binding decisions:

- FEMA Chief of Staff
- Associate Administrator, Mission Support
- Associate Administrator, Response and Recovery
- Deputy Administrator, Preparedness and National Protection
- FEMA Chief Financial Officer
- Associate Administrator, Federal Insurance and Mitigation Administration
- Associate Administrator, Office of Policy and Program Analysis
- Administrator, United States Fire Administrator
- Director, Office of Disability Integration & Coordination
- Chief Counsel, Office of Chief Counsel
- Chief Procurement Officer
- Chief Component Human Capital Officer
- Assistant Administrator, National Continuity Programs
- Regional Administrator Region III (or Deputy Regional Administrator)
- Regional Administrator Region VIII (or Deputy Regional Administrator)
- Regional Administrator, Region X (or Deputy Regional Administrator)
- Director, Office of Equal Rights
- 25% of the ITGB membership shall include GS-14 and GS-15 staff from Headquarters and Field Offices



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

FEMA respectfully requests that this recommendation be closed.

Recommendation 4: Implement a plan of action and milestones to address the integration and reporting limitations of existing systems.

Response: Concur. The IT Modernization Plan outlines initiatives which the FEMA ITGB has identified as necessary for modernization to be executed over the next five years. Each initiative is aligned with IT systems from the FEMA systems inventory, as well as investments that comprise FEMA's IT-53. Additionally, these initiatives incorporate business processes that align with and accommodate activities supporting new IT investments, governance board decisions, process changes, organization updates, system consolidation or other activities. An Integrated Project Team (IPT) was formed to complete each initiative (i.e. Grants Modernization, Financial Management Systems Modernization, Human Resource Information Systems, E-mail as a Service, National Flood Insurance Program, etc.). These IPTs are chartered to develop and execute a detailed implementation Plan of Action and Milestones (POAMs) to address the integration and reporting limitations of existing systems.

ECD: March 31, 2016.

Recommendation 5: Implement and enforce a standardized, agency-wide process that sufficiently defines and prioritizes the acquisition, development, operation, and maintenance requirements for all systems.

Response: Concur. FEMA will implement and enforce a standardized, agency-wide process that sufficiently defines and prioritizes the acquisition, development, operation, and maintenance requirements for all systems by exercising the following authorities through the ITGB:

- Approve all IT budget and investment requests;
- Certify that IT investments are adequately implementing incremental development;
- Review and approve any contract or other agreement for IT or IT services that are considered major investments; and,
- Define the development processes, milestones, review gates, and the overall policies for all capital planning, project management, and reporting for IT resources.

ECD: June 30, 2016

Again, thank you for the opportunity to comment on this draft report. Technical comments were previously provided under separate cover. Please contact Mr. Gary McKeon, FEMA's Audit Liaison Director, at 202-646-1308, should you have further questions. We look forward to working with you in the future.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix C

Office of Information Technology Audits Major Contributors to This Report

Richard Harsche, Deputy Assistant Inspector General

Steven Staats, Audit Manager

Elizabeth Argeris, Audit Manager

Craig Adelman, Senior Program Analyst

Chris Browning, Program Analyst

Barbara Bartuska, Independent Referencer

Pamela J. Chambliss-Williams, Independent Referencer



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix D Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.



OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305