

**FEMA's Longstanding
IT Deficiencies
Hindered 2017
Response and
Recovery Operations**





DHS OIG HIGHLIGHTS

FEMA's Longstanding IT Deficiencies Hindered 2017 Response and Recovery Operations

August 27, 2019

Why We Did This Audit

Information technology (IT) is a critical asset to support Federal Emergency Management Agency (FEMA) disaster response and recovery operations. We conducted this audit to assess the extent to which FEMA has implemented federally mandated IT management practices and identify challenges to ensuring FEMA's IT systems adequately support mission operations.

What We Recommend

We are making four recommendations to address FEMA's longstanding IT management and planning challenges, and better align IT resources with agency and mission priorities.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

FEMA has not implemented federally mandated IT management practices essential for effective oversight of its IT environment. Specifically, FEMA has not established an IT strategic plan, architecture, or governance framework to facilitate day-to-day management of its aging IT systems and equipment. We attribute these deficiencies to the FEMA Chief Information Officer's limited authority to manage IT agency-wide, as well as to a decentralized resource allocation approach that hinders funding for the centralized IT environment. These deficiencies are not new, and were reported in prior Office of Inspector General audits throughout the last 13 years. Continuation of this approach impedes budgeting for long-term IT enhancements, leads to overspending, and causes unnecessary IT support efforts.

Amid this management environment, FEMA has not provided its personnel with the IT systems necessary to support response and recovery operations effectively. FEMA's legacy IT systems are not integrated and lack the functionality needed to keep pace with high-volume processing. Additionally, the systems FEMA personnel rely on for situational awareness and emergency response coordination do not always contain real-time data nor do they support information sharing with external partners. We attribute these deficiencies to an inadequate focus on funding to support IT modernization efforts. As a result, field personnel engage in time-consuming, manual processes to accomplish mission tasks. For example, following the hurricanes and wildfires in 2017, some FEMA personnel used their personal laptop computers in place of FEMA's official systems to keep pace with mission requirements.

Management Response

FEMA concurred with our recommendations.

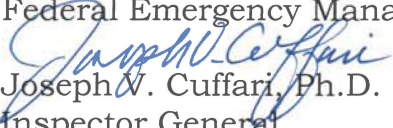


OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

August 27, 2019

MEMORANDUM FOR: Peter T. Gaynor
Acting Administrator
Federal Emergency Management Agency

FROM: 
Joseph W. Cuffari, Ph.D.
Inspector General

SUBJECT: *FEMA's Longstanding IT Deficiencies Hindered 2017
Response and Recovery Operations*

Attached for your information is our final report, *FEMA's Longstanding IT Deficiencies Hindered 2017 Response and Recovery Operations*. We incorporated the formal comments from the Associate Administrator, Office of Policy and Program Analysis, in the final report.

The report contains four recommendations aimed at improving FEMA's management of information technology. FEMA concurred with all four recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 through 4 open and resolved. Once FEMA 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.

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 Sondra McCauley, Assistant Inspector General, at (202) 981-6339.

Attachment: As stated.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Background 1

Results of Audit 6

 FEMA Has Not Implemented Mandated IT Management Practices 6

 FEMA Personnel Lacked the Technology Needed to Effectively Support
 Disaster Operations 17

Recommendations..... 26

Appendixes

Appendix A: Objective, Scope, and Methodology 31

Appendix B: FEMA Comments to the Draft Report 33

Appendix C: Status of Prior OIG Recommendations 38

Appendix D: FEMA’s Major IT Systems 41

Appendix E: Office of Audits Major Contributors to This Report 44

Appendix F: Report Distribution 45

Abbreviations

| | |
|-------|---|
| CIO | Chief Information Officer |
| EMMIE | Emergency Management Mission Integrated Environment |
| FEMA | Federal Emergency Management Agency |
| GAO | Government Accountability Office |
| IT | information technology |
| JFO | Joint Field Office |
| LSCMS | Logistics Supply Chain Management System |
| NEMIS | National Emergency Management Information System |
| OCIO | Office of the Chief Information Officer |
| OIG | Office of Inspector General |



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

The Federal Emergency Management Agency (FEMA) coordinates Federal Government activities to prepare for, prevent, respond to, and recover from domestic disasters, whether natural or manmade.¹ To accomplish its mission, FEMA has more than 12,000 employees working at headquarters offices in Washington, D.C., as well as 10 regional offices, 3 area offices, and more than 60 temporary disaster-related sites throughout the United States and its territories. Additionally, FEMA has more than 7,000 employees who remain on standby for deployment during disasters. For fiscal year 2018, FEMA had a budget of approximately \$17.3 billion, or 22 percent of the Department of Homeland Security's overall budget of \$70.7 billion.

FEMA takes a comprehensive approach to preparing for, responding to, and recovering from disasters, which involves partnerships and coordination across all levels of government. FEMA fosters partnerships with Federal, state, tribal, and local emergency management agencies, as well as non-governmental and private sector agencies that have disaster response and recovery responsibilities. FEMA's regional offices also help states and local communities conduct disaster planning and preparedness efforts to help minimize risks and allow for more rapid and efficient recovery. Personnel from the following FEMA offices carry out core mission operations. These offices are highlighted in the FEMA organization chart in figure 1.

- Response Directorate: Provides primary operational response needed to save and sustain lives and protect property in communities affected by natural disasters, acts of terrorism, or emergencies.
- Recovery Directorate: Provides recovery assistance to individuals, governments, and partner agencies affected by acts of terrorism, natural disasters, or emergencies.
- Logistics Management Directorate: Provides logistics capability to procure and deliver goods and services to support disaster survivors and local communities responding to and recovering from disasters.
- Field Operations Directorate: Coordinates rapid deployment of FEMA's field leadership and incident teams in response to disaster incidents.
- Federal Insurance and Mitigation Administration: Manages the National Flood Insurance Program and other programs designed to reduce future losses to homes, schools, public buildings, and critical facilities.

¹ FEMA's authority is derived from the *Disaster Relief Act of 1974*, Pub. L. No. 93-288, as amended by the *Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988*, Pub. L. No. 100-707.

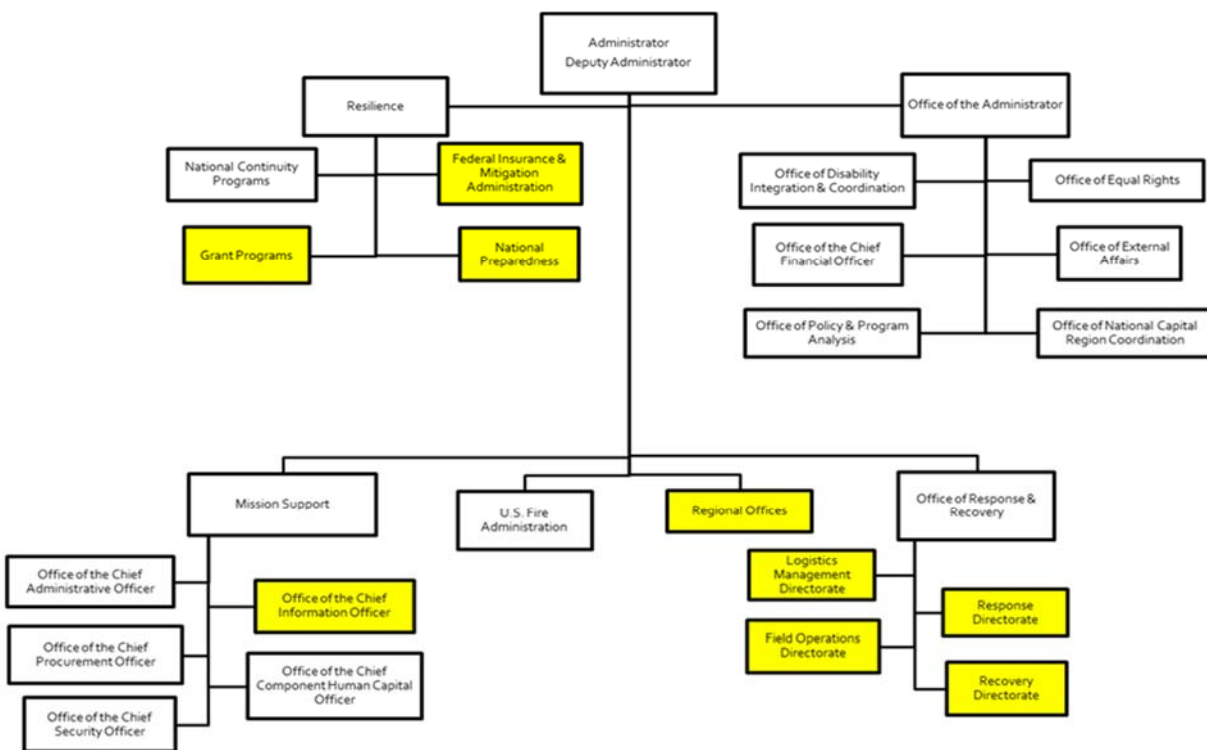


OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Grant Programs Directorate: Administers FEMA grants, including individual and public grants, and manages Federal assistance to improve capability and reduce risks during times of manmade and natural disasters.
- National Preparedness Directorate: Provides the doctrine, programs, and resources to prepare the Nation for preventing, responding to, and recovering from disasters.
- Office of the Chief Information Officer (OCIO): Housed under FEMA’s Mission Support Directorate, OCIO manages FEMA’s information technology (IT) infrastructure operations, including servers and networks; provides IT devices and software for use throughout FEMA; and oversees engineering and development of IT systems.

Figure 1: FEMA’s Organizational Structure



Source: DHS Office of Inspector General (OIG) analysis of FEMA data



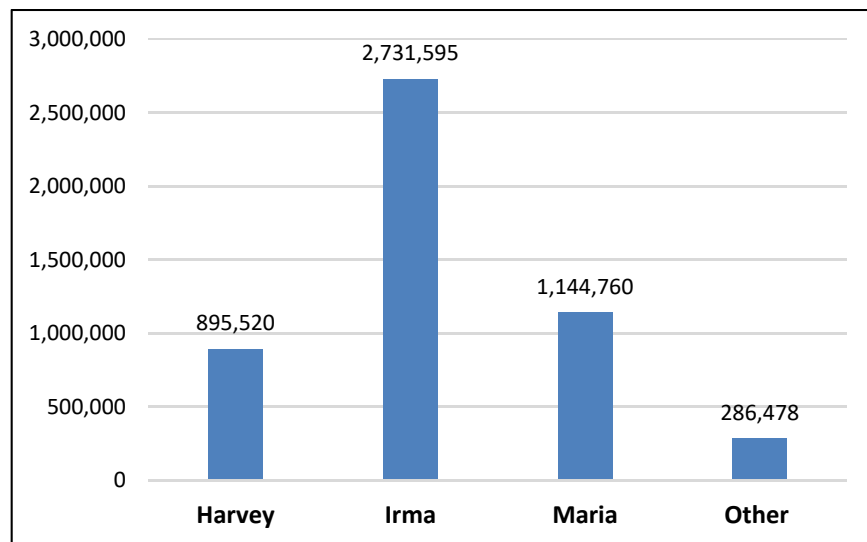
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

FEMA deploys thousands of employees from across its program offices to support response and recovery efforts following an incident or disaster. FEMA responded to an unprecedented number of major disasters during 2017. In total, FEMA supported 59 major disaster declarations, 16 emergency declarations, and 62 Fire Management Assistance Grant declarations affecting more than 35 states, tribes, and territories. Most notably, Hurricanes Harvey, Irma, and Maria resulted in extraordinary damage and destruction of critical infrastructure, livelihoods, and property. These hurricanes made landfall in the United States and its territories between August 25, 2017, and September 20, 2017, and were soon followed by devastating California wildfires that burned for months. Together, these disasters affected more than 47 million Americans — almost 15 percent of the U.S. population. FEMA obligated more than \$7.2 billion in disaster assistance in 2017. FEMA and its Federal partners provided 138 million meals, 194 million liters of water, 10.2 million gallons of fuel, and 1,310 generators to power critical facilities supporting survivors.

To illustrate the volume of work during this time, more disaster survivors registered for assistance in 2017 than in the previous 10 years combined. Figure 2 shows the total number of individual assistance grants applications submitted by survivors for open disaster declarations as of January 2018.

Figure 2: Total Applications for Individual Assistance as of January 2018



Source: DHS OIG analysis of FEMA data



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Technology Is Critical to Support FEMA’s Emergency Operations

The large-scale disasters of 2017 underscore the importance of technology for FEMA’s first responders and emergency management personnel to accomplish mission operations. Staff at all levels across FEMA depend on IT systems, equipment, and the underlying infrastructure to successfully complete their work. OCIO is responsible for managing the FEMA-wide IT infrastructure including servers, laptops, monitors, networks, printers, and all auxiliary hardware and software. OCIO also maintains enterprise IT services, such as networks, email, computers, and mobile devices used by FEMA employees, partner agencies, and disaster survivors. Additionally, OCIO is charged with establishing guidance and standards to increase efficiency and ensure FEMA workforce readiness. To accomplish this, OCIO manages a staff of more than 500 full-time personnel located at headquarters and field locations, and an additional 330 temporary employees who deploy to the field to perform response and recovery activities following disasters or emergencies.

FEMA maintains hundreds of IT systems and databases that deliver essential capabilities during response and recovery operations and throughout the year. Table 1 shows the primary systems that support FEMA’s mission requirements.

Table 1: Key FEMA Systems by Mission Area

| Response and Recovery Systems | |
|---|---|
| Web-based Emergency Operations Center | A crisis management system that provides a real-time common operating picture for FEMA headquarters, regions, and Federal, state, local, and tribal partners. |
| National Emergency Management Information System (NEMIS) | FEMA’s primary platform to support all phases of emergency management and disaster-assistance decision making, and serve as FEMA’s official system of record for storing emergency management files. |
| Enterprise Data Warehouse | A central repository of data replicated from other systems and used to perform analysis, summarization, and emergency management duties. The system also generates reports on the status of emergency management and financial programs, projects, and funding. |
| Grants Systems | |
| Grants Manager | Used to process and track public assistance grants after an area receives a Federal declaration. Applicants also use the system to manage status and activities related to grant claims. |
| Emergency Management Mission Integrated Environment (EMMIE) | Used to obligate funding for public assistance grants after a disaster is recorded in NEMIS. |



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

| | |
|--|--|
| Non-Disaster Grants Management System | Used to process and manage non-disaster grant applications. |
| Logistics System | |
| Logistics Supply Chain Management System (LSCMS) | Manages the supply chain of disaster assets, resources, and commodities for FEMA and partner agencies and organizations. |
| Financial System | |
| Web-Integrated Financial Management Information System | FEMA's official financial management system used to record, track, and report on all of FEMA's financial transactions. |

Source: DHS OIG analysis of FEMA data

We have issued four audit reports since 2005 highlighting the Chief Information Officer's (CIO) inability to ensure FEMA's IT environment effectively supported critical mission needs. We reported that FEMA had not adequately planned and managed its IT, and its systems were not integrated, nor did they allow for data sharing or reporting to keep pace with mission operations. Appendix C provides a summary of our prior audit findings and the status of our recommendations.

The Government Accountability Office (GAO) has drawn similar conclusions through a number of audits of FEMA's IT management. In November 2017, GAO reported that FEMA needed to take additional action to fully satisfy system development, testing, and integration of its new public assistance grants tracking system.² Similarly, in April 2016, GAO reported that FEMA faced challenges with IT governance and oversight, modernization, workforce planning, and ensuring its IT programs adequately support disaster response activities.³ In its December 2008 report, GAO identified FEMA's challenges with sharing information among Federal, state, and local participants in the public assistance grants process, as well as tracking the status of projects.⁴

² *Opportunities to Enhance Implementation of the Redesigned Public Assistance Grant Program*, GAO-18-30, November 2017

³ *FEMA Needs to Address Management Weaknesses to Improve Its Systems*, GAO-16-306, April 2016

⁴ *FEMA's Public Assistance Grant Program Experienced Challenges with Gulf Coast Rebuilding*, GAO-09-129, December 2008



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Results of Audit

FEMA has not implemented federally mandated IT management practices essential for effective oversight of its IT environment. Specifically, FEMA has not established an IT strategic plan, architecture, or governance framework to facilitate day-to-day management of its aging IT systems and equipment. We attribute these deficiencies to the FEMA CIO's limited authority to manage IT agency-wide, as well as to a decentralized resource allocation approach that hinders funding for the centralized IT environment. These deficiencies are not new, and were reported in prior OIG audits throughout the last 13 years. Continuation of this approach impedes budgeting for long-term IT enhancements, leads to overspending, and causes unnecessary IT support efforts.

Amid this management environment, FEMA has not provided its personnel with the IT systems necessary to support response and recovery operations effectively. FEMA's legacy IT systems are not integrated and lack the functionality needed to keep pace with high-volume processing. Additionally, the systems FEMA personnel rely on for situational awareness and emergency response coordination do not always contain real-time data nor do they support information sharing with external partners. We attribute these deficiencies to an inadequate focus on funding to support IT modernization efforts. As a result, field personnel engage in time-consuming, manual processes to accomplish mission tasks. For example, following the hurricanes and wildfires in 2017, some FEMA personnel used their personal laptop computers in place of FEMA's official systems to keep pace with mission requirements.

FEMA Has Not Implemented Mandated IT Management Practices

FEMA has not fulfilled statutory requirements to develop an IT strategic plan and an enterprise architecture as a foundation for enterprise-wide IT guidance and standards. Both management practices are essential for effective oversight of FEMA's IT investments and operating environment. We attribute these deficiencies to the FEMA CIO's limited oversight authority and FEMA's decentralized allocation of IT funding directly to program offices, which has hindered long-term IT budgeting, caused inefficient IT spending, and resulted in unnecessary workloads, particularly during the 2017 disaster season.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Key Management Activities Needed to Manage IT Agency-wide

Although mandated for all Federal agencies more than 20 years ago, FEMA has not implemented two essential IT management practices — strategic planning and enterprise architecture development — both necessary to effectively guide IT resources. FEMA also lacks a mature framework for governing IT investment decisions agency-wide.

Lack of a Strategic Plan to Guide IT Management Activities

Federal agency CIOs are required to conduct strategic planning activities to identify and document how IT will be used to accomplish each agency's mission.⁵ DHS supports these requirements by directing its component CIOs to develop, implement, and maintain up-to-date IT strategic plans each year.⁶ An IT strategic plan is critical for an agency like FEMA, with an aging and complex IT environment. The need is especially critical for effective tools and technologies to help carry out its response and recovery responsibilities.

Despite these requirements, FEMA has not published an IT strategic plan for more than six years. Between 2011 and 2013, FEMA's OCIO developed at least four IT planning documents, which included goals, objectives, and IT performance metrics.⁷ However, FEMA did not effectively execute or follow through on finalizing these IT plans due to shifting priorities and insufficient resources. Without an IT strategic plan, FEMA cannot effectively identify how it will leverage new technology to reduce operational complexity, increase efficiency, and improve mission outcomes.

The absence of an IT strategic plan undermines FEMA's ability to carry out the agency-wide goals and objectives recently published in FEMA's 2018 strategic plan. The 2018 plan highlights the agency's need to accelerate its technology modernization efforts. One of the plan's three strategic goals is aimed at simplifying processes and procedures across FEMA's technology environment.⁸ Notably, the third goal in the 2018 plan calls for actions to decommission outdated legacy IT systems and develop innovative systems and business practices to enable employees to achieve the agency's mission. Figure 3 highlights the objectives and actions focused on improving FEMA's IT environment.

⁵ OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 28, 2016

⁶ DHS Directive 142-02, Revision 01, *Information Technology Integration and Management*, April 12, 2018

⁷ *FEMA 2013–2016 Technology Management Strategic Plan; FEMA IT Strategic Plan FY 2013–2016; FEMA OCIO 2013–2014 Annual Plan; and FEMA OCIO Business Transformation Project: Findings and Recommendations*

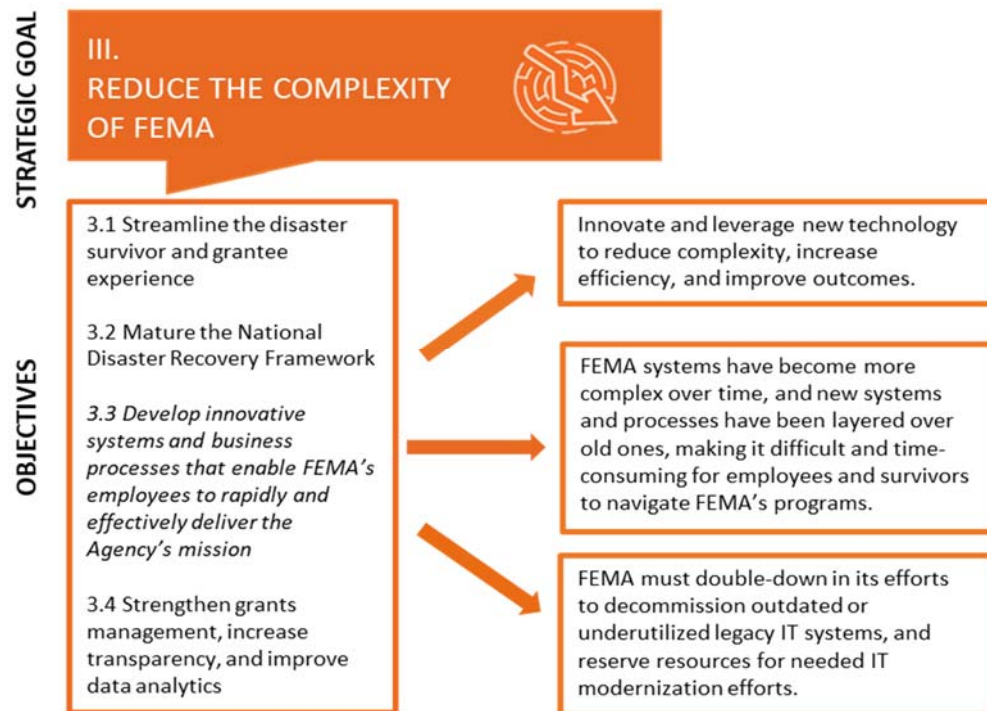
⁸ *Federal Emergency Management Agency 2018–2022 Strategic Plan*



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 3: IT-Related Objectives from FEMA’s Strategic Plan



Source: DHS OIG-generated based on the *Federal Emergency Management Agency 2018 – 2022 Strategic Plan*

Until the FEMA CIO develops a strategic plan for managing and modernizing its IT, FEMA program offices may lack assurance that the current IT environment can meet their urgent mission needs. In the interim, FEMA offices and directorates have developed their own internal plans to manage IT activities at the program level. For example, in 2017, FEMA’s Office of Response and Recovery created its *Disaster Emergency Communications 5-Year Program Plan*. This plan provided an end-state assessment of FEMA’s Response Directorate and regional operating requirements through 2022. Similarly, the Recovery Technology Programs Division created an IT-specific modernization strategy in 2018 to address the need for cost-effective and efficient systems to support the needs of Recovery Directorate programs.

Inadequate Enterprise Architecture and IT Standards

Federal laws dating more than 20 years ago require Federal agencies to define and document all enterprise-wide IT systems, data, and business functions.⁹ This comprehensive inventory is known as an enterprise architecture.

⁹ *Clinger-Cohen Act of 1996* (40 U.S. Code 11101 *et seq.*) and *Federal Information Security Management Act of 2002*, Pub. L. No. 107-347, tit. III



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

When implemented properly, an enterprise architecture provides a foundation for enterprise-wide IT guidance and standards.

The FEMA OCIO lacks an up-to-date repository of all pre-approved software and hardware available to FEMA personnel, which is a key element for building an enterprise architecture. The existing repository, known as the FEMA Technical Reference Model, was established more than 15 years ago but has not been maintained or kept current. In December 2018, FEMA discontinued using the repository and transitioned to a web-based DHS-wide Technical Reference Model system. However, FEMA personnel told us the Technical Reference Model used in 2017 did not include tools essential for FEMA's response and recovery work, such as mobile and wireless devices, external hardware, and removable storage.

An enterprise architecture and IT repository are precursors to providing the guidance and standards for ensuring the readiness of FEMA's distributed workforce at headquarters and field locations. However, significant work remains for FEMA to provide this guidance, which is essential to field personnel's ability to install quickly the needed IT equipment in Joint Field Offices (JFO) and Disaster Recovery Centers during fast-paced mission operations. Standards are lacking for pre-approved networks, workstations, printers, servers, and cables. Associated access controls for guest wireless and trusted network access are also missing. Staffed with only four employees, FEMA's Enterprise Architecture Team has been inadequate to maintain the repository or inventory of FEMA's IT environment. In 2017, the team reduced its support of standard initiatives such as IT acquisition reviews and disaster-related Technical Reference Model updates, because staff were deployed to the field to support Hurricane Harvey operations.

We previously reported in 2005 that FEMA had not successfully implemented an enterprise architecture to govern its IT environment.¹⁰ Similarly, in 2011 we again disclosed that significant work remained for FEMA to develop a complete agency-wide architecture.¹¹ At that time, the OCIO planned to complete a baseline architecture by 2012, but its efforts were hindered by staffing and funding shortages.

¹⁰ *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery*, OIG-05-36, September 2005

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



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Insufficient Framework for Governing IT Investment Decisions

Federal laws dating back to 1996 require agencies to implement overarching governance structures that enable effective management of IT resources, including IT projects and investments.¹² Agencies are mandated to establish policies and procedures for conducting investment reviews, operational analyses, or other performance reviews to evaluate IT resources. More recently, since 2014, agencies are also required to ensure their CIOs have a significant role in IT management, governance, and oversight processes.¹³ Specifically, CIOs are required to approve IT budget requests, certify that IT investments adequately implement the incremental development process, and conduct annual IT portfolio reviews.¹⁴

Despite these mandates, FEMA has not implemented a governance framework to ensure consistent and coordinated management of its IT resources. The foremost element of such a framework is a centralized IT decision-making body to make investment decisions. FEMA instituted an IT Governance Board in February 2012; however, just 1 year later, the CIO deemed the board ineffective because it did not meet regularly and did not have a sound approach for assessing potential IT projects. In 2014, the FEMA CIO revised the charter to better define governance board processes and expected outcomes. However, during our audit fieldwork in August 2018, senior FEMA officials said the board was still not operating as an agency-wide IT decision-making body due to infrequent meetings and ineffective vetting of IT investment decisions.

Lack of CIO Authority and Funding to Improve IT Management

We attribute FEMA's continuing lack of progress in instituting effective IT management practices to two primary factors. First, FEMA leadership has not given the CIO adequate authority to plan and manage IT resources agency-wide. Second, FEMA's decentralized approach of allocating funds directly to program offices results in fewer resources for support entities such as OCIO. Perpetual de-prioritization of long-term IT planning in favor of disaster-related activities indicates that FEMA leadership does not view IT improvement as a management priority.

¹² *Clinger-Cohen Act of 1996*

¹³ *Federal Information Technology Acquisition Reform Act*, Pub. L. No. 113-291, div. A, tit. VIII, subtit. D

¹⁴ Incremental development of IT systems promotes continuous adaptive planning, development, testing, and delivery/integration, and encourages rapid and flexible response to change.



OFFICE OF INSPECTOR GENERAL

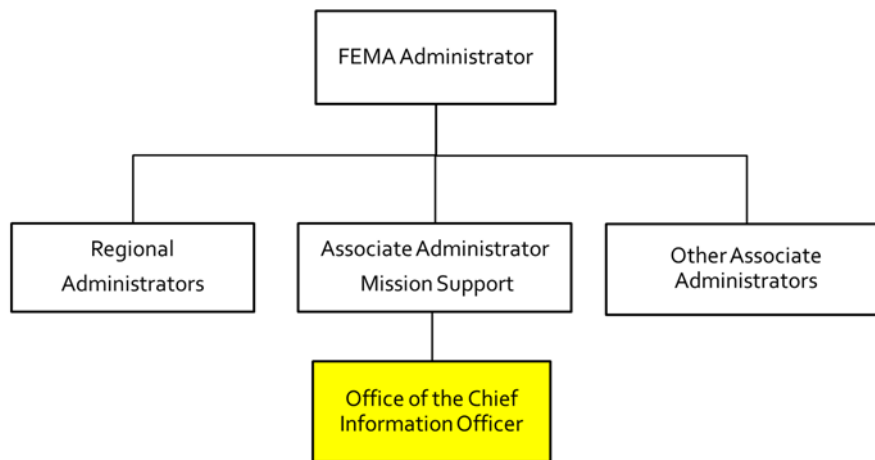
Department of Homeland Security

Lack of CIO Authority for Agency-wide IT Management

FEMA leadership has not given the CIO adequate authority to oversee and manage IT efforts agency-wide. According to Federal law, CIOs must be positioned with authority to improve the operating efficiency of their agencies and deliver enterprise-wide solutions.¹⁵ Such authority was re-emphasized in a 2018 Executive Order calling for enhanced ability of CIOs to better position agencies to modernize their IT systems and execute IT programs more efficiently.¹⁶ Therefore, each CIO must be empowered by the agency head with authority for IT governance, resources, and oversight. Ideally, the agency CIO would report directly to the agency head.

Despite these requirements, the authority of FEMA's CIO is impeded by its reporting position within the organizational structure. Rather than reporting directly to the FEMA Administrator, the CIO reports to the Associate Administrator for Mission Support, who reports to the Administrator, as shown in figure 4.

Figure 4: FEMA CIO Position



Source: DHS OIG analysis of FEMA data

Due to this indirect reporting relationship, the CIO lacks central oversight of agency-wide IT assets and programs. FEMA personnel rely on more than 300 IT systems and databases to conduct day-to-day work. However, very few of these systems are under the CIO's direct control. The CIO has authority over only 22 OCIO-owned systems out of 97 major FEMA IT systems. FEMA program offices independently manage the remaining 75 systems. Appendix D includes a list of FEMA's major IT systems.

¹⁵ *Clinger-Cohen Act of 1996; Federal Information Technology Acquisition Reform Act*

¹⁶ Executive Order 13833, *Enhancing the Effectiveness of Agency Chief Information Officers*, May 15, 2018



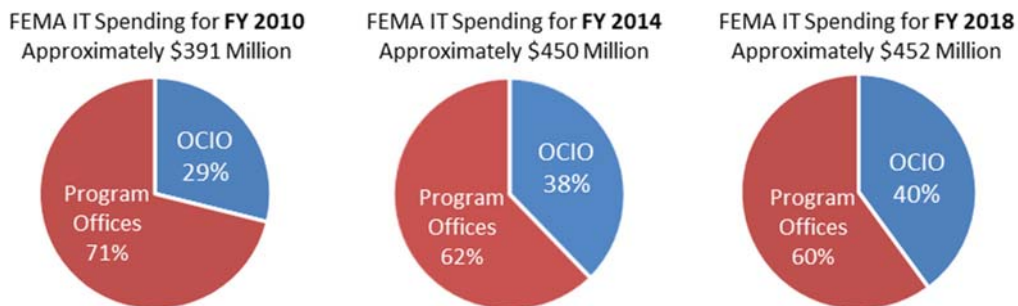
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Similarly, FEMA program offices maintain independent IT budgets and spending authority, while the CIO only controls OCIO-level spending for support purposes such as managing FEMA’s IT infrastructure and maintaining enterprise IT services. For example, FEMA’s FY 2018 IT spending totaled more than \$452 million; however, only about 40 percent of this amount was under the CIO’s purview. Decentralized management of funds leaves the CIO without visibility of program office IT spending and the ability to plan for effective agency-wide support. As a result, the OCIO has struggled to balance unplanned IT spending for operations, maintenance, and cybersecurity against long-term system upgrades and modernization efforts.

FEMA’s decentralized IT funding approach has not changed for the last eight years, leaving the CIO with insufficient resources and authority to effectively manage FEMA’s IT environment. In 2011 and 2015, we reported the OCIO’s IT budget routinely accounted for only one-third of total IT spending, with FEMA program offices accounting for the remaining two-thirds.¹⁷ For example, in FY 2010, FY 2014, and FY 2018, program offices were granted authority over 71 percent, 62 percent, and approximately 60 percent of the IT budget, respectively, as shown in figure 5. Although OCIO IT spending increased nominally during this period, the CIO continues to lack sufficient and proportionate funding to modernize legacy systems and improve outdated infrastructure. Additionally, a senior OCIO official said more than 70 percent of FEMA’s annual IT budget supports aging infrastructure and remediation of vulnerabilities, leaving less than 30 percent for investing in modernization efforts to improve mission support capabilities.

Figure 5: Program vs. OCIO IT Spending



Source: DHS OIG analysis of FEMA data

¹⁷ *FEMA Faces Challenges in Managing Information Technology*, OIG-16-10, November 2015



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Decentralized Resource Allocation Approach Hinders Funding for IT Improvement

FEMA's decentralized approach of allocating resources directly to each program office has been a major obstacle to ensuring funding to improve FEMA's overall IT environment. Under this approach, mission-focused programs are able to direct-hire IT specialists to support program office IT rather than rely on OCIO-provided, centralized IT support. This has resulted in program offices growing internal IT support staffs that commonly outnumber OCIO staff levels. For example, as of August 2018, FEMA had 1,183 IT personnel. However, less than 50 percent, or 518, of those positions reported to the OCIO. The other 665 IT positions reported to program and field offices that maintained their own IT support operations to meet internal demands. For example, the Recovery Directorate maintained a staff of approximately 150 to support its own IT development and maintenance activities. Officials from this directorate also augmented IT staff with contractor personnel to meet program office needs.

Longstanding staffing challenges further hinder OCIO's ability to carry out required IT planning and management functions. As of August 2018, the OCIO had staffed about 50 percent, or approximately 260, of its total 518 approved positions. Inadequate OCIO staffing has been an ongoing challenge for a number of years. In 2011, we identified staffing shortages as a hindrance to the OCIO's ability to complete critical work such as documenting its business functions, information resources, and IT systems, as well as institutionalizing its baseline IT enterprise. In 2014, the OCIO had not staffed 150 of 594 approved positions. According to a senior official, many OCIO personnel have departed for new jobs or retirement, but positions were not back-filled with permanent employees. For example, staff in the OCIO's Office of Planning, Architecture and Governance decreased in 2017, delaying work on modernizing systems and infrastructure and on managing FEMA's capital planning and investment control program.

OCIO staffing shortages were compounded in 2017, when 85 percent of OCIO staff were deployed to support field operations following a series of devastating disasters, including the hurricanes that made landfall in the United States and its territories. Within the OCIO organization, 50 percent of the Enterprise Architecture Branch staff was deployed for many months, delaying the branch's ability to manage day-to-day work such as processing Change Advisory Board requests and supporting Technical Reference Model modernization initiatives for the OCIO.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

IT Not Viewed as a Senior Management Priority

The OCIO's limitations are evident each year, as FEMA leadership routinely prioritizes disaster-focused activities over proactive and strategic-level IT planning and management. We disclosed this in a 2018 management alert, in which we concluded FEMA leadership had not been able to carry out corrective actions to improve longstanding IT management challenges because of its competing mission priorities.¹⁸ Moreover, we noted that FEMA leadership had withheld the funding and staff that OCIO divisions needed to address our prior report recommendations effectively.

Over time, OCIO leadership has sought additional resources and authority to address IT management deficiencies, but without success. We spoke with several senior OCIO officials who recounted specific, ongoing efforts to address outstanding OIG report recommendations related to IT management. During the past 13 years, we have issued 4 reports on FEMA's IT challenges, including 20 recommendations to address longstanding technology and management deficiencies. These recommendations are listed in appendix C. In response to our reports, FEMA leadership acknowledged the need for change and modernization of its IT enterprise; however, it has yet to take appropriate actions to resolve many of the critical challenges previously identified. Many of the IT management issues we identified in our 2005, 2011, and 2015 reports remained unchanged up to the time of our current fieldwork, concluding in September 2018.

IT Management Deficiencies Led to Unanticipated Costs and Workloads

The FEMA CIO's inability to effectively plan long-term has led to reactionary and excess IT spending. Also, in the absence of a completed enterprise architecture and accompanying IT standards and guidance, personnel faced additional and unanticipated workloads to support critical response and recovery operations during the 2017 disaster season.

Unanticipated IT Costs Due to Inability to Plan Long-term

Without an IT strategic plan, architecture, or centralized governance approach to guide effective IT decision making, the CIO is unable to plan and budget long-term for agency-wide IT needs. This has resulted in uncoordinated, uninformed, and reactionary IT spending that routinely surpasses approved levels. FEMA's FY 2018 IT spending of more than \$452 million exceeded the

¹⁸ *Management Alert—Inadequate FEMA Progress in Addressing Open Recommendations from our 2015 Report, "FEMA Faces Challenges in Managing Information Technology,"* OIG-18-54, February 2018



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

approved IT budget by approximately \$56 million. Covering the excess expenses required ad hoc reprogramming of OCIO and program office budget items and reallocation of funding from other IT initiatives. For example, program offices routinely used end-of-FY funds to develop IT systems, but did not coordinate with OCIO to track costs for future-year upkeep and maintenance. This resulted in unplanned OCIO funding requirements. Senior officials we interviewed described the budget process as a repetitive, impromptu shifting of funds to accommodate IT initiatives deemed higher priorities by FEMA- or program-level leadership. An OCIO director said funding allocated to her division had been diverted to pay for other IT priorities, which diminished her capacity to complete requirements, such as investment management and modernization planning.

A lack of centralized authority also prevents the CIO from maintaining adequate visibility of IT development and maintenance costs incurred by each program office year-to-year. In 2017, FEMA's regional offices, JFOs, Disaster Recovery Centers, and other temporary field locations routinely created and implemented local IT tools or solutions without OCIO awareness or oversight. For example, during the establishment of a Disaster Recovery Center following Hurricane Harvey in 2017, IT personnel circumvented the requirement for OCIO review of IT-related purchases by acquiring 19 wireless network routers costing \$19,800, which fell below the \$20,000 threshold that triggers a required formal contracting process.

Workforce Readiness Hindered by a Lack of IT Standards and Guidance

FEMA's success begins with the readiness of its disaster workforce. However, absent a fully developed enterprise architecture as a basis, the OCIO has been unable to provide adequate guidance or standards to support FEMA's various field locations. The effects of this deficiency were most obvious in 2017 when field offices and recovery centers needed to be established quickly to support disaster response operations. For example, following Hurricane Harvey, FEMA did not have an approved system in place for wireless network access, so IT staff spent several weeks installing more than 80 miles of network cable and wiring approximately 1,200 connections for workstations and other devices. IT infrastructure set-up has historically been a cause for delays in opening field facilities following disasters. Figure 6 shows network set-up efforts at a JFO in Texas.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security



Figure 6: JFO Network Set-up Following Hurricane Harvey
Source: FEMA

Unfortunately, the network configuration was insufficient to support the growing number of disaster surge workforce and other personnel at the JFO. To augment the existing infrastructure, field IT staff worked to implement a wireless network to support additional users office-wide. However, FEMA did not have an approved standard for field wireless networks, so IT staff lacked specific guidance for establishing JFO Wi-Fi service. Soon after implementation, OCIO deployed additional personnel to the field office to certify use of the wireless network solution and validate its compliance with network security standards.

The lack of IT guidance delayed the onboarding process for the disaster surge workforce deployed to the field in 2017. FEMA deployed more than 17,000 personnel, including more than 4,000 non-FEMA federal employees, to support the 2017 disaster response and recovery operations. However, the mobilization centers responsible for issuing IT equipment did not have adequate instructions on establishing network and systems access for non-DHS personnel. Field sites also lacked guidance and a standard process for issuing mobile devices, such as tablets and cellular phones, to the surge workforce. FEMA procures its mobile devices from commercial vendors, such as Apple Corporation, which require that deployed personnel have individual accounts for access and use. However, when deployed personnel return devices to FEMA without deactivating their accounts, the devices become locked and require factory re-set by the vendor. IT personnel at numerous field locations spent many hours working with Apple representatives to individually re-set each locked device, resulting in unplanned costs and lost productivity. An official we spoke with stated that he received a box full of locked devices for issuance to



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

surge workforce personnel. The official had to work directly with Apple customer service to re-set each device individually before it could be issued. This delayed the deployment of more than 100 people to perform urgent disaster fieldwork.

FEMA Personnel Lacked the Technology Needed to Effectively Support Disaster Operations

FEMA's IT systems do not provide personnel with the functionality they need to conduct disaster response and recovery activities. FEMA's inability to address longstanding system deficiencies is due to limited IT budget allocations. As a result, personnel engaged in inefficient, time-consuming workarounds or relied on their own personal devices to accomplish urgent tasks. Working in this manner increases the risk that disaster assistance and grants could be delayed and duplication of benefits could occur.

IT Systems Lacked Functionality Necessary to Accomplish Mission Tasks

It is essential that FEMA personnel have adequate IT systems to support their critical work during high-tempo mission operations. Federal law requires agencies to acquire, use, and manage IT to improve mission performance.¹⁹ Similarly, DHS policy directs component CIOs to ensure that enterprise IT services and solutions are available to support agency personnel.²⁰ Yet, FEMA's IT environment remains ineffectively complex, as many of its systems are not sufficiently integrated and lack critical functionality to process claims, maintain situational awareness, or share information with stakeholders during disaster response and recovery operations.

Non-integrated Systems Did Not Support Efficient Data Tracking and Exchange

FEMA personnel identified IT complexity as a major barrier to successfully carrying out timely emergency management operations. The most notable challenges stemmed from a lack of integration among some of FEMA's emergency management systems. For example, processing public assistance grants required personnel to enter data separately into two non-integrated systems (EMMIE and Grants Manager). Personnel also used NEMIS and the financial management system to request and process grant funding allocations.

¹⁹ *Paperwork Reduction Act of 1995*, Pub. L. No. 104-13; *Clinger-Cohen Act of 1996* (40 U.S. Code 11101 *et seq.*)

²⁰ DHS Instruction 142-02-001, *Information Technology Integration and Management*, March 4, 2015

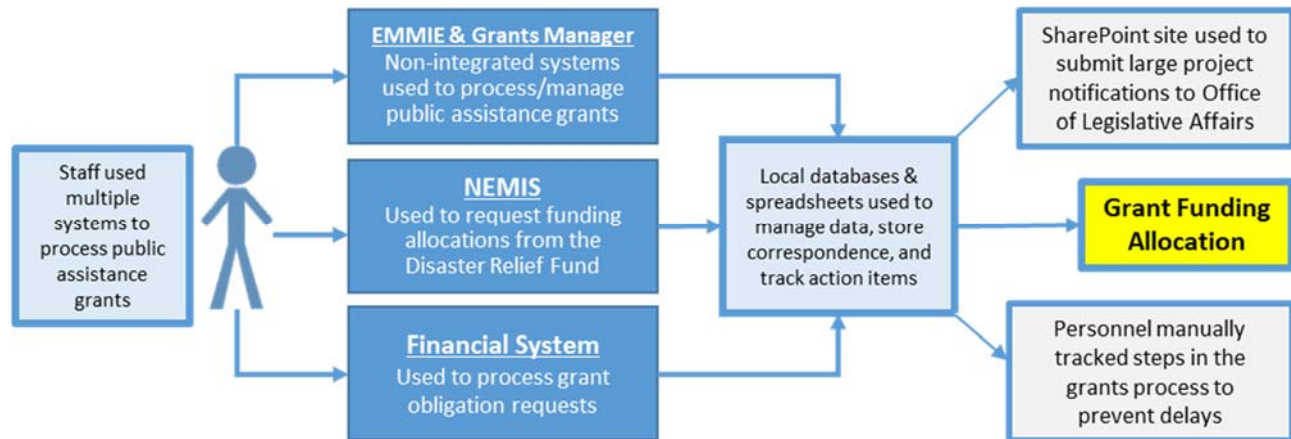


OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Grants personnel at numerous regional and field offices relied on spreadsheets, SharePoint sites, and local databases to overcome challenges associated with using non-integrated systems to manage grant cases, as shown in figure 7.

Figure 7: Public Assistance Grants Processing



Source: DHS OIG re-creation based on statements by FEMA personnel

FEMA received more than 17,000 public assistance grants applications in 2017. However, systems used to manage public assistance grants were incapable of performing critical functions like identifying multiple funding allocations for the same grant, which could result in duplicate payments to applicants. To prevent this, grants staff from a regional office had to manually review each grant in multiple systems to verify that duplicate funding requests were not submitted. This systematic inefficiency resulted in grant disbursement delays of 8 months or longer in that region.

The lack of systems integration prevented efficient tracking and management of individual grants. To ensure complete information on an individual grant, personnel had to continually monitor progress separately in each system and manually notify stakeholders when additional actions were required. For example, regional office staff used spreadsheets to track event information, such as notifications to FEMA’s comptroller office on funding allocations, because the systems did not send alerts to take action when needed. Apart from manual tracking and notifications by regional grants staff, timely action could not be completed by comptroller staff and other stakeholders.

Similarly, FEMA grants processing personnel had to rely on two separate systems to manage preparedness grant period of performance, which is the expected timeframe for a grantee to complete grant activities and expend approved funds. Preparedness grants are intended to enhance the capacity of



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

state and local emergency responders to prepare for threats. However, because the primary preparedness grants system, the Non-Disaster Grants Management System, was not integrated with FEMA's financial management system, personnel had to manually add data separately in both systems to complete each grant project.

Field locations that provided disaster support during 2017 faced similar IT system challenges. JFO staff supporting Hurricane Harvey response operations recounted the need to use as many as five separate systems to request IT equipment for field offices. For example, standard-issue IT equipment, such as laptops, printers, and network circuits, are pre-staged at FEMA's Disaster Information Systems Clearinghouse for distribution to field locations supporting response and recovery operations. Orders for pre-staged IT assets are submitted through FEMA's Network Inventory and Optimization Solutions system. Then a separate system, the Sunflower Asset Management System, is used to track the exact location of equipment distributed to the field. Personnel used a different system, the Enterprise Coordination and Approval Processing System, to submit and process requisitions for IT equipment that was not readily available. FEMA personnel told us they were confused as to which system they should use for which purpose. Staff also said they faced delays of up to 2 weeks to receive much-needed IT equipment and services during Hurricane Harvey disaster response operations.

We observed similar conditions during our prior FEMA audit work and have made numerous recommendations for FEMA to address these issues. In 2005 and 2011, we reported that FEMA response and recovery systems were not integrated internally and did not effectively support information exchange during disaster mission operations. We similarly disclosed that FEMA grants management systems were not integrated or linked to the systems of external stakeholders. In 2015, we reported again that critical systems were not sufficiently integrated to support operations. For example, we identified FEMA's crisis management system was not integrated with two other systems required to complete mission assignments processing, prompting the need to enter the same information into all three systems.

Systems Did Not Provide Adequate Situational Awareness

Maintaining situational awareness of emergency response efforts is essential for FEMA personnel to effectively aid survivors, coordinate with state and local partners, and support decision making. However, FEMA personnel faced significant challenges accessing real-time information in FEMA's data warehouse, which is used to perform a wide range of emergency management duties. FEMA personnel told us the data warehouse performed as expected following Hurricane Harvey; however, in the aftermath of Hurricanes Irma and



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Maria several weeks later, information in the data warehouse became unavailable for up to 6 weeks. This occurred because a higher volume of users performing simultaneous response and recovery tasks placed heavy demand on the system, causing significant slowness as disaster information transmitted from IT systems to the data warehouse. The slowness delayed the transmissions to the data warehouse by up to 90 hours, as data from all systems was processed in the order it was received. Survivor applications for individual assistance alone spiked from an average of more than 28,000 per day during the first 2 weeks following Hurricane Sandy in 2012, to as many as 150,000 per day following Hurricanes Harvey, Irma, and Maria during August and September 2017. A lack of real-time information in the data warehouse had a significant effect on FEMA's ability to perform critical work. Personnel in several regions stated this slowed the processing of hundreds of thousands of individual assistance applications for disaster survivors who had suffered damage or loss to their personal property.

The lack of up-to-date information in the data warehouse hindered FEMA's communication and coordination with its stakeholders. For example, FEMA typically receives numerous requests for information from partner agencies, the media, and Congress during disasters. These requests include inquiries about response and recovery activities, grant funding or processing, and survivor requests for congressional assistance or intervention. To respond to these inquiries, personnel need timely access to a variety of information such as grant funding obligation reports, budget execution plans, state grant data calls, and survivor assistance totals.

FEMA logistics personnel also rely on real-time information to strengthen their situational awareness during disaster response operations. However, the system they used to track logistics supply chain status (LSCMS) did not always provide real-time data to ensure visibility and support coordination of supplies and commodities to disaster survivors and communities. For example, LSCMS tracking of data on commodities like meals and water delivered to Puerto Rico lagged behind the real-time data reported to FEMA headquarters. A regional response official said that, like the data warehouse, LSCMS performed as expected following Hurricane Harvey, but later experienced delays in data availability due to heavy demands on the system following Hurricanes Irma and Maria.

The delayed data availability caused a need for hard-wired network connections, since existing wireless networks lacked the bandwidth required to operate LSCMS. Logistics personnel in the field had to manually record tracking data until they could enter it into LSCMS after returning to network-connected locations at a later time. For example, personnel used spreadsheets to track common planning data, such as the movement and locations of empty



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

shipping trailers. The high volume of manual processing outside of LSCMS adversely affected data accuracy, caused confusion among staff about available assets and stock, and wasted time during critical response operations.

We issued similar findings in our previous audit work. Specifically, in 2005 we reported that FEMA systems did not provide staff with real-time capabilities for tracking deployments of personnel, equipment, and supplies. In 2008, we reported that FEMA did not have real-time awareness of logistics activities to track its supplies.²¹ In 2011, we concluded that FEMA was still challenged to track supplies or ensure real-time visibility of supply chain activities across multiple logistics systems.

Systems Did Not Allow for Critical Information Storage or Sharing

FEMA personnel lacked an enterprise solution for storing disaster information, which can amount to many terabytes of data. FEMA personnel at every field office we visited said managing high volumes of data collected during disaster response and recovery operations is a foremost challenge every year. Without an official, agency-wide information repository, personnel managed files differently at each field office and location. For example, staff saved files across various local network shared drives, a local SharePoint site, or within more than a dozen other FEMA systems. Working in this manner caused confusion and delays, as FEMA personnel could not easily locate data when needed for reporting and responding to impromptu data calls. For example, a regional official supervising grants management said staff could not readily respond to data calls from the California Office of Emergency Services without first submitting queries in multiple systems and then spending extra time manually reviewing and tallying the information to provide accurate results.

FEMA personnel did not have an approved file transfer solution, such as a file transfer protocol or file hosting application, to share large data files with their internal and external partners. Sharing timely information with stakeholders is critical for effective planning, resource allocation, and overall decision-making to manage incident response across government organizations. For example, state partners need to have FEMA response and recovery information on missing persons, reported fatalities, rescue operations, and community damage assessments to carry out their complementary emergency management responsibilities. This type of information may include large video files containing footage of rescue operations, graphics files, maps, or photography that are often too large to transfer through FEMA's email service.

²¹ *Logistics Information Systems Need to Be Strengthened at the Federal Emergency Management Agency*, OIG-08-60, May 2008



OFFICE OF INSPECTOR GENERAL

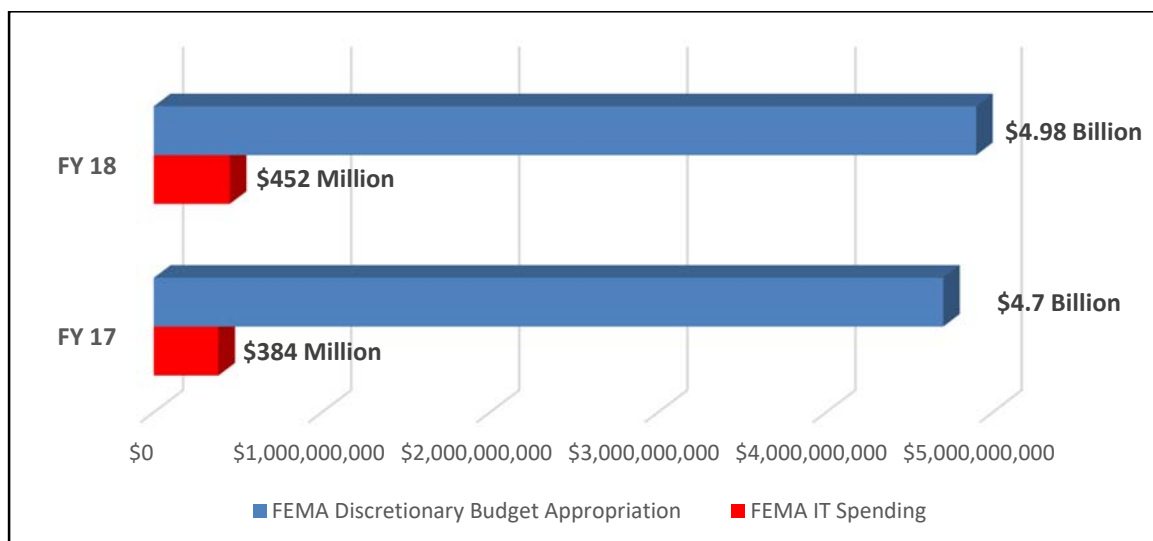
Department of Homeland Security

Without an approved file transfer solution, personnel in multiple regions had to circumvent FEMA’s enterprise network to deliver video files to FEMA offices or other stakeholders. For example, following Hurricane Irma, personnel in one FEMA regional office coordinated with the Department of Defense to use “DivX,” a commercial system, to compress large files for transfer to FEMA headquarters.²² In another example, officials from the City of Houston requested housing-related data on approximately 400,000 of its residents following Hurricane Harvey. Regional staff could not send attachments through FEMA’s email service due to data size restrictions of 50 megabytes. To provide the requested information, regional staff coordinated with FEMA’s Reporting and Analytics Division and the FEMA OCIO to arrange use of the U.S. Army’s Safe Access File Exchange system.

IT Budget Constraints Hindered Efforts to Address Systems Challenges

FEMA’s ability to address these longstanding IT system deficiencies is constrained due to budgetary limitations. According to OCIO and program office officials, FEMA’s annual IT spending of less than \$500 million represents less than 10 percent of FEMA’s \$4.98 billion discretionary budget. Funding has historically fallen short of the amount needed to modernize FEMA’s IT enterprise while continuing to support routine IT operations and maintenance. Figure 8 shows FEMA’s annual budget and IT spending for FYs 2017 and 2018.

Figure 8: FEMA’s Annual Budget and IT Spending for FYs 2017 and 2018



Source: DHS OIG analysis of DHS and FEMA data

²² DivX is a commercial brand of video products that has the ability to compress lengthy video segments into small sizes while maintaining high visual quality.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The OCIO is also hampered by increasing costs to support FEMA's outdated IT environment, which supersedes funding for systems modernization. We found at least 70 percent of FEMA's \$396 million IT budget for FY 2018 had been obligated to support FEMA's aging IT infrastructure. As a result, the OCIO was not able to implement major efforts to update legacy IT systems or improve systems capabilities. The OCIO estimated that approximately 70 percent of FEMA IT assets were functioning beyond end-of-life standards and more than 80 percent of FEMA's core network infrastructure and disaster infrastructure equipment was 10 to 20 years old and needed to be upgraded or replaced.

FEMA uses the Disaster Relief Fund to support its disaster-related work. This is a separate appropriation FEMA can use to fund eligible response and recovery efforts associated with major disasters and emergencies. For example, disaster relief funding can be used to purchase IT equipment and services in direct support of disaster-based operations. However, policy governing the use of disaster relief funding restricts its use only to authorized Federal disaster support activities.²³ FEMA cannot use the Disaster Relief Fund for non-disaster expenses such as annual IT costs or long-term IT modernization initiatives.

Unless FEMA places priority on increasing its annual IT spending allocation, it will likely remain unable to effectively plan or budget for much-needed systems improvements and modernization initiatives across its IT enterprise.

Field Personnel Relied on Manual Workarounds and Unauthorized Equipment

As a result of system limitations, FEMA personnel engaged in inefficient, time-consuming workarounds, or relied on their personal IT accounts and devices to accomplish urgent tasks. Working in this manner introduces the potential for data errors and exposes FEMA's network and IT infrastructure to security risks while increasing the potential for delays or duplication of disaster assistance and grants payments.

Manual Workarounds Were Prevalent

During our fieldwork, we met with 285 staff members from FEMA field locations, nearly all of whom said they were stymied by IT-related challenges while performing disaster response and recovery work. At each field site we visited, FEMA personnel expressed concern and frustration with the local solutions and workarounds they had to devise and use daily to complete required work. A number of them recounted that workarounds had been a necessary practice for several years, given FEMA's longstanding IT deficiencies.

²³ FEMA Directive 125-7, *Financial Management of the Disaster Relief Fund*, October 1, 2016



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Manual workarounds or ad hoc processes may suffice during minor and short-term events; however, they could not effectively sustain the increased workload and information-sharing requirements following the series of major disasters in 2017. For example,

- Following Hurricane Harvey in August 2017, more than 900 personnel were deployed to the field to help survivors with disaster assistance registrations. These personnel gathered survivor information using a mobile application; however, the application was often unavailable due to insufficient capacity to support the extremely high volume of users. To overcome this frequent challenge, field staff had to complete their work during off-hours when system use decreased. Field teams purchased commercial maps to track where they had gone each day, since such data could not be recorded during periods when the system was unavailable. This location data had to be keyed in when FEMA's reporting tool became available for use. The widespread problems with system availability resulted in field officials directing teams to recanvas areas already visited, which wasted time and caused delays in collecting survivor registrations, responding to case inquiries, and reporting case updates.
- Following Hurricane Irma in September 2017, JFO staff in Florida used a Microsoft Access database and at least 20 spreadsheets to manage temporary housing data for local survivors. This became necessary early during response operations when FEMA's emergency management information system (NEMIS) proved incapable of effectively tracking application data and other specific housing information, resulting in inaccurate reporting and a need for data adjustments. To address this problem, staff used a central dashboard to enter data outside of NEMIS. Staff also used spreadsheets to log data such as trailers ready for occupancy and site inspection results. Performing this work outside of NEMIS led to even more inaccurate and inconsistent housing data, which resulted in misreporting at national daily briefings that adversely affected field office credibility. Additionally, the field office's ability to make informed planning decisions, identify supply and demand, and authorize individual housing solutions during Hurricane Irma response operations was impaired.
- Regional personnel also faced major challenges completing non-disaster-related tasks. For example, personnel devised their own tools to compensate for critical functionality gaps in FEMA's non-disaster grants management system. Specifically, the system lacked a closeout module, which meant that all closeout activity had to be processed and completed separately. Managing closeout activities apart from the system resulted



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

in staff working additional hours to properly manage the period of performance for each grant project. Grants specialists said they had created hundreds of spreadsheets over time to manage data for a grant lifecycle, including recording events such as amendments that occur each time a grantee draws funding from a grant.

Unauthorized Personal Equipment Used to Avoid Work Delays

Because FEMA-issued IT equipment and systems did not adequately support mission requirements, field personnel routinely relied on their own personal devices and equipment to complete simple, yet critical, tasks. At every site we visited, personnel disclosed the need to use personal equipment, private accounts and applications, or commercially-available resources to complete critical disaster work such as editing video footage of response and recovery operations, sharing large data files with external stakeholders, and establishing network access. Personal equipment included laptop computers, Bluetooth devices, cellular phones, external monitors, and removable storage drives. However, personal devices may not meet DHS security requirements and are typically not authorized in the Technical Reference Model for use with FEMA systems.²⁴ An IT supervisor who worked at a Hurricane Maria disaster location said that staff depended on personal devices daily to complete their work.

FEMA field staff also relied on personal accounts or applications to share or transfer large files, create video footage and photographs, and perform work in remote locations lacking system or network access. For example, employees at various locations said they had to use personal log-ins for applications like Google Drive to transfer or share large data files, including video footage and photographs, to FEMA headquarters offices and other internal and external stakeholders. An official supporting response operations following Hurricane Harvey said he had to use his personal laptop and Google Drive account to send information on survivors and damaged areas to the JFO. Without access to personal devices and account services, employees would have been unable to share critical information or perform time-sensitive work to accomplish mission operations.

In addition, FEMA did not have adequate wireless networks to support response and recovery operations, especially in remote field locations. Personnel used personal devices to complete work, which introduced potential security vulnerabilities to FEMA's infrastructure and network systems. For example, following one 2017 hurricane, staff working at a JFO set up wireless hotspots using personal mobile phones to establish wireless network access for FEMA computers. In some situations, wireless connections were so poor that

²⁴ DHS Sensitive Systems Policy Directive 4300A, Version 13.1, July 27, 2017



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

supervisors instructed staff to work from their hotel rooms for improved wireless access using the hotel network service. In other cases, personnel relied on public Wi-Fi service at commercial facilities, like fast food restaurants, to perform required work. FEMA personnel said at times, this was the only option for employees working in remote field locations to complete required work.

Conclusion

FEMA must be flexible and adaptable to respond to evolving threats, support the needs of individuals and communities, and work effectively with partners and stakeholders. To successfully achieve its mission, FEMA must modernize its IT systems and infrastructure to make response and recovery operations more efficient, and to deliver assistance in as simple a manner as possible. However, effective IT planning activities, such as establishing an IT strategic plan and enterprise architecture, are necessary to guide much-needed IT modernization efforts. FEMA must address these longstanding deficiencies to coordinate IT development activities effectively across its program and regional offices to ensure that IT investments are supporting FEMA's mission and priorities. In this management environment, the CIO has been unable to identify and budget for long-term consolidation, integration, or automation efforts. Without progress in these areas, personnel will remain dependent on outdated and unintegrated legacy systems, inadequate equipment, and alternative solutions, such as manual workarounds and unauthorized equipment, to accomplish critical disaster response and recovery operations.

Recommendations

We recommend the Acting Administrator, Federal Emergency Management Agency:

Recommendation 1: Provide the Office of the Chief Information Officer with the necessary authority and resources to implement required IT management practices in accordance with Federal mandates.

Recommendation 2: Promote IT planning and management as an agency-wide priority by establishing a policy to implement and enforce a centralized IT investment management framework.

Recommendation 3: Direct a strategic planning effort to define FEMA's vision for IT, along with a funding plan, to demonstrate how FEMA will direct investments to better align IT resources with agency and mission priorities.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We recommend the Chief Information Officer, Federal Emergency Management Agency:

Recommendation 4: Develop a systems modernization approach that includes a plan for resolving IT integration, information sharing, and reporting deficiencies.

OIG Analysis of FEMA Comments

We obtained written comments on a draft of this report from the Associate Administrator, Office of Policy and Program Analysis. In the comments, the Associate Administrator, Office of Policy and Program Analysis, provided details on FEMA's extensive support for first responders and emergency management personnel, IT governance, and data management. We have included a copy of the comments in their entirety in appendix B.

We reviewed FEMA's comments, as well as the technical comments previously submitted by FEMA under separate cover, and made changes to the report as appropriate. The Associate Administrator, Office of Policy and Program Analysis, concurred with all of our recommendations. The following is our evaluation of FEMA's response to our recommendations.

Recommendation 1: We recommend the Acting Administrator, Federal Emergency Management Agency, provide the Office of the Chief Information Officer with the necessary authority and resources to implement required IT management practices in accordance with Federal mandates.

Management Comments

The Associate Administrator, Office of Policy and Program Analysis, concurred and stated the FEMA Acting Administrator signed a directive delegating authority to the FEMA CIO to exercise and fulfill IT responsibilities for FEMA. The delegation includes the authority to plan and manage FEMA's portfolio of IT investments and resources in coordination with an executive-level panel, to carry out all programmatic delivery aspects of FEMA's IT investments, and to develop IT budgets and IT expenditure plans in coordination with other responsible parties. FEMA's OCIO has also begun developing a capabilities analysis report to inform decisions for reducing technical complexity, improving cost effectiveness, and appropriately resourcing IT management. FEMA expects to complete these efforts by May 31, 2020.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG Analysis

We recognize FEMA's approach of formally delegating authority to the CIO and completing a capabilities analysis report to inform IT decision making as positive steps toward addressing this recommendation. We look forward to receiving further updates on the implementation of these initiatives. This recommendation is open and resolved.

Recommendation 2: We recommend the Acting Administrator, Federal Emergency Management Agency, promote IT planning and management as an agency-wide priority by establishing a policy to implement and enforce a centralized IT investment management framework.

Management Comments

The Associate Administrator, Office of Policy and Program Analysis, concurred and stated FEMA established an OCIO Policy Working Group to guide consistent and integrated development and revision of OCIO policy documents, such as the IT portfolio management framework. The OCIO is also working on pragmatic implementation of the roles and responsibilities for IT investment management within its offices and across agency organizations that have local authority for their own IT purchases and budget. Further, OCIO intends to strengthen IT governance by revising its governance board scope and membership, and ensuring key technology decisions are made by the board based on the portfolio framework. FEMA expects to complete these efforts by June 30, 2020.

OIG Analysis

We recognize FEMA's efforts to improve and integrate IT development, revise OCIO policy documents, and strengthen IT governance across FEMA as positive steps toward addressing this recommendation. We look forward to receiving updates, along with documentary evidence, as these plans are completed and implemented. This recommendation is open and resolved.

Recommendation 3: We recommend the Acting Administrator, Federal Emergency Management Agency, direct a strategic planning effort to define FEMA's vision for IT, along with a funding plan, to demonstrate how FEMA will direct investments to better align IT resources with agency and mission priorities.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Management Comments

The Associate Administrator, Office of Policy and Program Analysis, concurred and stated OCIO is currently drafting an IT strategic plan for 2019–2023. The plan is expected to address ongoing challenges, provide additional oversight of IT investment decisions, ensure coordination and execution of IT plans, promote effective IT governance, and outline strategies for modernizing systems.

Concurrent with this effort, OCIO is developing an implementation plan to detail OCIO initiatives intended to align key IT funding resources, including staff, to support FEMA’s vision, goals, and objectives. Both documents will be reviewed by other IT mission and business stakeholders to ensure the technology backbone of FEMA’s day-to-day operations can provide flexible and reliable support to FEMA programs. FEMA expects to complete these plans by May 31, 2020.

OIG Analysis

We recognize FEMA’s approach of drafting an IT strategic plan and implementation plan as a positive step toward addressing this recommendation. We look forward to receiving updates on implementation and execution of these plans. This recommendation is open and resolved.

Recommendation 4: We recommend the Chief Information Officer, Federal Emergency Management Agency, develop a systems modernization approach that includes a plan for resolving IT integration, information sharing, and reporting deficiencies.

Management Comments

The Associate Administrator, Office of Policy and Program Analysis, concurred and stated FEMA’s new data sharing directive and implementation plan outline steps toward more informed decisions and improved mission execution by ensuring data is better able to support responders. Data sharing, reporting, and management initiatives, including the Enterprise Data and Analytics Modernization Initiative, are being led by FEMA’s Office of Policy and Program Analysis. To address challenges in this area, FEMA plans to maximize internal data sharing, integration, and interoperability; promote data sharing with the public; and develop a plan for creation of a Chief Data Officer. The OCIO will work in conjunction with the Office of Policy and Program Analysis to document, communicate, and educate internal and external stakeholders and partners on data sharing tools, procedures, and security requirements to



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

enable more efficient and effective mission delivery. FEMA expects to complete these efforts by April 30, 2020.

OIG Analysis

We recognize FEMA's efforts and plans to resolve data-related challenges as positive steps toward resolving this recommendation. We look forward to receiving additional details and documentation on these efforts, including results of implementation and projections regarding future outcomes. 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 (Pub. L. No. 107-296)* by amendment to the *Inspector General Act of 1978*. We conducted this audit to assess the extent to which FEMA has implemented IT management practices mandated for Federal agencies and to identify challenges to ensuring FEMA's IT systems adequately support disaster response mission operations.

To conduct this audit, we researched and used Federal, departmental, and agency criteria related to Federal IT management requirements. We obtained and reviewed published reports and other relevant documents, testimonial transcripts, and media articles related to FEMA's management and use of IT. Additionally, we reviewed GAO and DHS OIG reports to identify previous findings and recommendations related to FEMA's management of IT.

We held more than 60 meetings and interviewed more than 300 FEMA personnel at headquarters and field locations, as well as personnel from external stakeholder agencies and offices. At FEMA headquarters, we interviewed the Associate Administrator for Mission Support, the Acting CIO, and the Acting Deputy CIO. We met with senior officials from FEMA's Office of the Chief Financial Officer, Office of the Chief Procurement Officer, Office of Response and Recovery, National Preparedness Directorate, Federal Insurance and Mitigation Administration, Grants Programs Directorate, and National Flood Insurance Program. We talked with personnel from specialized support offices, such as the Recovery Analytics Division and the Disaster Information Systems Clearinghouse. Finally, we spoke with senior officials, IT supervisors, and system users from FEMA's Pacific Area Office at Honolulu, Hawaii; Long-Term Recovery Offices at Austin, Texas, and Guaynabo, Puerto Rico; and Joint Field Offices at Orlando, Florida, and Sacramento, California.

We visited FEMA Region IV in Atlanta, Georgia; Region VI in Denton, Texas; and Region IX in Oakland, California. We also went to the Texas Recovery Office Branch in Houston, Texas. During these visits, we interviewed executives and supervisory personnel, IT specialists, and support personnel/end users. We met with representatives from the Texas Division of Emergency Management to assess the effectiveness of FEMA's IT systems from a state agency perspective. We also collected and analyzed supporting documentation about FEMA's IT environment, IT management practices, system challenges, and improvement initiatives. We also observed system use during normal operations.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We conducted this performance audit between May and September 2018 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.



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

August 8, 2019

MEMORANDUM FOR: Joseph V. Cuffari
Inspector General

FROM: Joel Doolin *joel a doolin*
Associate Administrator
Office of Policy and Program Analysis

SUBJECT: Management Response to OIG Draft Report: "FEMA's
Longstanding IT Deficiencies Hindered 2017 Response
and Recovery Operations"
(Project No. 18-084-ITA-FEMA)

Thank you for the opportunity to review and comment on this 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.

As recognized in the draft report, FEMA responded to an unprecedented number of major disasters in 2017, resulting in more disaster survivors registering for assistance than during the previous 10 years combined. FEMA is committed to supporting first responders and emergency management personnel to accomplish their mission with the necessary Information Technology (IT) systems and support. This OIG audit aligns with FEMA's current areas of focus including improvements in leadership and accountability, IT portfolio management, application of enterprise architecture, and oversight of IT resources including governance.

Though 2017 challenged FEMA in many ways, the Agency also had many successes in support of our first responders and emergency management personnel, governance, and data management. For example, during Hurricanes Harvey, Irma, and Maria, FEMA successfully established a Wireless FEMA Enterprise Network that supported multiple disaster field offices. This initiative allowed FEMA staff at multiple disasters to connect to the enterprise network quickly and securely without needing a dedicated wired connection and proved to be not only more efficient, but also more cost effective.

FEMA's Office of the Chief Information Officer (OCIO) has also advanced its integration with FEMA's resource planning process. In 2019, the IT Investment Management Council analyzed program budget requests and made



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

recommendations to the Deputy Administrator, as Chair of the Program and Budget Executive Panel, in support of the Fiscal Year 2021-2025 Resource Allocation Plan. To improve the utility of the tools used to understand approved technology, FEMA OCIO leveraged DHS tools and also published a Disaster Products Guide for operations in the field.

In addition, FEMA recently issued a Data Sharing Directive and Implementation Plan to work in concert with the existing Data Management Directive, which established the framework for how FEMA builds capability and capacity to effectively manage data as an asset. Both Directives align with the 2019 President's Management Agenda priority for "Data, Accountability, and Transparency." These are part of FEMA's efforts to take deliberate steps to support information sharing both within the agency and with external partners in secure and efficient ways.

The draft report contained four recommendations with which FEMA concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Attachment: Management Response to Recommendations Contained in OIG 18-084-ITA-FEMA

The OIG recommended that the Acting Administrator, FEMA:

Recommendation 1: Provide the OCIO with the necessary authority and resources to implement required IT management practices in accordance with Federal mandates.

Response: Concur. On February 12, 2019, the FEMA Acting Administrator signed Delegation Number 0106-12, which delegates authority to the FEMA Chief Information Officer (CIO) to exercise and fulfill IT responsibilities for FEMA. The Delegation includes the authority to plan and manage the FEMA portfolio of IT investments and resources in coordination with an executive-level panel, to carry out all programmatic and delivery aspects of FEMA's IT investments, and to develop IT budgets and IT expenditure plans in coordination with other responsible parties.

To fully understand agency-wide infrastructure modernization and capability requirements needed to support infrastructure and management, FEMA's OCIO has also begun developing a Capabilities Analysis Report (CAR). The purpose of the CAR is to define the infrastructure baseline, determine overall technical and management capabilities, and document and address management practices needed to implement the capability gaps. The CAR will inform decisions related to reducing technical complexity, improving cost effectiveness, and appropriately resourcing IT management. After the CAR is developed, the program will follow the Joint Requirements Integrated Management System process. Estimated Completion Date (ECD): May 31, 2020.

Recommendation 2: Promote IT planning and management as an agency-wide priority by establishing a policy to implement and enforce a centralized IT investment management framework.

Response: Concur. During March 2019, FEMA established a newly-formed OCIO Policy Working Group to guide the consistent and integrated development and revision of OCIO policy-related documents. The group meets regularly to coordinate policy and guidance to help ensure OCIO activities, functions, and processes are adequately integrated. The working group is focused on strengthening policy gaps and is currently overseeing the update of the IT Integration and Management Directive (FD-140-2) to better clarify the authorities for IT planning and management, along with the roles and responsibilities of program managers, directorates, and staff throughout FEMA.

It is important to note that FEMA is fully compliant with all U.S. Department of Homeland Security Capital Planning Investment Control (CPIC) reporting requirements. However, FEMA is still planning to revise its IT portfolio management framework and supporting processes to better incorporate the use of CPIC data in the select, control and evaluate



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

phases of its framework. The revised framework will better address gaps in enforcing centralized IT investment management. This revised framework will be detailed in the forthcoming IT portfolio management instruction.

Under the direction of FEMA's recently appointed CIO, the OCIO is working on pragmatic implementation of the roles and responsibilities for IT investment management within its offices and across agency organizations that have localized authority over their own IT purchases and budget. To strengthen IT investment portfolio management, OCIO is strengthening IT governance by revising its governance board scope and membership, and ensuring key technology decisions are made by the board based on the portfolio management framework. ECD: June 30, 2020.

Recommendation 3: Direct a strategic planning effort to define FEMA's vision for IT, along with a funding plan, to demonstrate how FEMA will direct investments to better align IT resources with agency and mission priorities.

Response: Concur. Under the direction of the new CIO, the OCIO is currently drafting the FEMA IT Strategic Plan for 2019-2023. The Plan will outline FEMA's IT vision, mission, and the supporting goals and objectives that will focus the efforts of FEMA IT towards Agency and mission priorities. The Plan will focus on ensuring that steps are taken towards ongoing challenges, including providing more oversight of IT investment decisions, coordinating and executing IT plans, implementing effective IT governance, and modernizing our systems.

Concurrent with this effort, OCIO is developing a tactically-focused OCIO implementation plan. This plan will detail the OCIO initiatives that are intended to align key IT funding resources, including staff, in support of the overall Agency's vision, goals and objectives. Both documents will be reviewed within OCIO and by other IT mission and business stakeholders, such as program and regional offices, to ensure the critical technology backbone of our day-to-day operations can provide the flexible and reliable support needed by FEMA programs. To exercise the plan, OCIO will outline methods for directing IT investments in alignment with strategy. This will be done through redefining and exercising the IT Governance Board. ECD: May 31, 2020.

Recommendation 4: Develop a systems modernization approach that includes a plan for resolving IT integration, information sharing, and reporting deficiencies.

Response: Concur. FEMA's new Data Sharing Directive and Implementation Plan outlines steps toward more informed decisions and improved mission execution by ensuring data is better able to support responders. Data sharing and data management initiatives including reporting are being led by FEMA's Office of Policy and Program Analysis (OPPA) with the Enterprise Data and Analytics Modernization Initiative. To address challenges in this area, FEMA will maximize internal data sharing, integration, and



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

interoperability; maximize data sharing with the public; and, develop a plan for the creation of a Chief Data Officer.

OCIO will work in conjunction with OPPA to document, communicate, and educate internal and external stakeholders and partners on data sharing tools, procedures and security requirements to enable more efficient and effective mission delivery. ECD: April 30, 2020.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C
Status of Prior OIG Recommendations

| Report | Recommendation | Current Status |
|--|---|---------------------------------------|
| <p>OIG-05-36: <i>Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery</i>, September 2005</p> <p>Key Findings:</p> <ul style="list-style-type: none"> Alignment of FEMA’s IT with DHS’ strategic direction would prove challenging; CIO support of IT users could be improved; FEMA systems were not integrated and did not effectively support information exchange during response and recovery operations; and FEMA had not updated its enterprise architecture to govern its IT environment. | 1. Update the FEMA strategic plan to support achievement of DHS goals and ensure that all FEMA systems provide the performance data necessary to measure progress toward achieving response and recovery goals; and, subsequently update the IT strategic plan in line with the updated FEMA strategic plan. | Closed |
| | 2. Ensure that personnel, through the Emergency Preparedness and Response Directorate training division, receive adequate systems training, guidance, and communication needed to support disaster response and recovery activities effectively. | Closed |
| | 3. Complete the FEMA enterprise architecture, linked to the department-wide architecture and ongoing initiatives that may impact Emergency Preparedness and Response Directorate operations. | Closed |
| | 4. Ensure cross-cutting participation from headquarters, regions, and states in processes to develop and maintain a complete, documented set of FEMA business and system requirements. Additionally, analyze alternatives and determine the most appropriate approach to providing the technology needed to support these business and system requirements. | Closed |
| | 5. Develop and maintain a testing environment that duplicates the real systems environment and ensures that all systems components are properly and thoroughly tested prior to their release. Additionally, ensure that proper configuration management activities are followed and documented. | Closed |
| <p>OIG-08-60: <i>Logistics Information Systems Need to Be Strengthened at the Federal Emergency Management Agency</i>, May 2008</p> | 1. Finalize logistics, strategic, and operational plans to guide logistics activities. | Administratively Closed ²⁵ |
| | 2. Develop, communicate, and implement standardized processes and procedures for logistics activities. | Administratively Closed |
| | 3. Evaluate current IT systems to determine their ability to support logistics operations. | Administratively Closed |

²⁵ All four of the recommendations from our report OIG-08-60 were administratively closed based on new audit work that began in 2010, not based on completion of corrective actions.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

| | | |
|---|---|--|
| <p>Key Findings:</p> <ul style="list-style-type: none"> FEMA’s IT systems were not integrated to support asset management; and FEMA did not effectively support logistics activities by providing limited visibility of disaster-related shipments. | <p>4. Develop a strategy for acquiring IT systems to support the logistics mission.</p> | <p align="center">Administratively Closed</p> |
| <p>OIG-11-69: <i>Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology</i>, April 2011</p> <p>Key Findings:</p> <ul style="list-style-type: none"> FEMA did not have a comprehensive IT strategic plan with clearly defined goals, objectives, or guidance for program office initiatives; FEMA had not documented its enterprise architecture; OCIO did not understand IT resources and needs throughout the agency; and Efforts to modernize critical systems had been put on hold due to departmental consolidation plans. | <p>1. Develop a comprehensive IT strategic plan with clearly defined goals and objectives to support program IT initiatives.</p> | <p align="center">Closed</p> |
| | <p>2. Complete and implement a FEMA enterprise architecture to establish technical standards and guidelines for systems acquisitions and investment decisions.</p> | <p align="center">Closed</p> |
| | <p>3. Establish and maintain a complete, comprehensive enterprise IT systems inventory.</p> | <p align="center">Closed</p> |
| | <p>4. Establish an agency-wide IT budget planning process to include all FEMA program technology initiatives and requirements.</p> | <p align="center">Closed</p> |
| | <p>5. Obtain agency-wide IT investment review authority to ensure that all IT initiatives and systems development efforts align with FEMA’s mission.</p> | <p align="center">Closed</p> |
| | <p>6. Establish a consolidated modernization approach for FEMA’s mission-critical IT systems, to include DHS plans for integrated asset management, financial, and acquisition solutions.</p> | <p align="center">Administratively Closed²⁶</p> |
| <p>OIG-16-10: <i>FEMA Faces Challenges in Managing Information Technology</i>, November 2015</p> <ul style="list-style-type: none"> FEMA developed IT planning documents, but did not effectively coordinate or execute on those plans; | <p>1. Finalize necessary IT planning documents that reflect the current IT strategy of the organization and IT modernization initiatives.</p> | <p align="center">Open</p> |
| | <p>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.</p> | <p align="center">Open</p> |
| | <p>3. Finalize the IT governance board charter and expand the capacity of the board to</p> | <p align="center">Closed</p> |

²⁶ Recommendation 6 from our report OIG-11-69 was administratively closed based on new audit work that began in 2014, not based on completion of corrective actions.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

| | | |
|--|---|------|
| <ul style="list-style-type: none">FEMA improved its IT governance by establishing an IT Governance Board but results had not been fully effective; andFEMA's IT systems were not integrated and did not provide personnel with data search and reporting tools for meeting operational needs. | make the board the IT decision-making authority for the agency. | |
| | 4. Implement a plan of action and milestones to address the integration and reporting limitations of existing systems. | Open |
| | 5. Implement and enforce a standardized, agency-wide process that sufficiently defines and prioritizes the acquisition, development, operation, and maintenance requirements for all systems. | Open |



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix D
FEMA's Major IT Systems

| OCIO-owned Systems |
|--|
| Authentication and Provisioning Services |
| Document Management and Records Tracking System |
| Electronic Fingerprint System |
| Enterprise Applications Development Integration Sustainment Beta |
| Enterprise Applications Development Integration Sustainment |
| Enterprise Coordination and Approval Process System |
| Enterprise Data Warehouse |
| Enterprise Shared Workspace |
| Enterprise Wireless LAN |
| FEMA Employee Knowledge Center |
| FEMA Enterprise Network |
| FEMA Office 365 System |
| FEMA Support System |
| FEMA Virtual Desktop Infrastructure |
| FEMA Virtualized Data Center |
| FEMA Workstations |
| Headquarters Enclave |
| Mobility Environment for FEMA |
| Network Inventory and Optimizations Solution |
| PACS Physical Access Control System |
| Service Oriented Architecture |
| Test and Development LAN |
| Program Office-owned Systems |
| Acquisition Package |
| Assistance to Firefighters Grants |
| Automated Construction Estimating Software System |
| Center for Domestic Preparedness Learning Management System |
| Center for Domestic Preparedness Local Area Network |
| Chemical Stockpile Emergency Preparedness Program (Portal) |
| Chemical Stockpile Emergency Preparedness Program (WebCA) |
| Chemical Stockpile Emergency Preparedness Program (Emergency Operations Planning Tool) |
| Citizen Corps |
| Community Information System |
| Contact Center Capability Modernization Program |
| Crisis Management System |



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

| |
|---|
| Customer Satisfaction Analysis System |
| Deployment Tracking System |
| Disaster Assistance Improvement Program |
| Disaster Emergency Communication |
| Disaster Management Support Environment Cloud Environment |
| Electronic Document/Records Management System |
| Electronic Workforce Management |
| Emergency Notification System |
| Emergency Operations Center Network |
| Emergency Support |
| Emergency Support Functions 6 Support System |
| Environmental and Historic Preservation Management Information System |
| Facilities Management System |
| FEMA Applicant Case Tracker (also known as PA Grants Manager) |
| FEMA Electronic Discovery Litigation Software |
| FEMA National Radio System |
| FEMA Response Coordination Center |
| First Responder Training |
| Grants Reporting Tool |
| Hazard Mitigation Grant Program |
| Individual Assistance |
| Integrated Public Alert and Warning System |
| Logistics Supply Chain Management System |
| Map Service Center |
| Mapping Information Platform – Data Center 2 |
| Mapping Processing and Analysis Center |
| Mitigation eGrants |
| National Distribution Center |
| National Emergency Management Information System – Emergency Coordination |
| National Emergency Training Center Local Area Network |
| National Fire Incident Reporting System |
| National Flood Insurance Program Information Technology Systems |
| National Public Warning System |
| National Radio Network |
| National Flood Insurance Program Direct Servicing Agent |
| National Flood Insurance Program Virtual Information Technology System |
| Non-Disaster Grants Management System |
| Payment and Reporting System for Grantees |
| Preparedness Toolkit |
| Region Audio Video System |



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

| |
|---|
| Region Geospatial Information System |
| Region IV Application Development and Test Environment |
| Region IV Digital Signage |
| Region IV Public Wireless Local Area Network |
| Region IX Audio Video System |
| Region IX Disaster Workforce Transformation Initiative |
| Region IX Southern California Area Field Office Coordination Center |
| Region Local Area Network |
| Region VI Web Server Farm |
| Region Virtualized Environment |
| Region Wireless Local Area Network |
| Region X Emergency Response Unified Planning Tool |
| Region X Facility Management System |
| Regional Watch Center |
| System Integration Test |
| Training.fema.gov |
| United States Fire Administration Systems |
| United States Fire Administration Web Farm |
| Virginia Systems Repository |
| Web-Integrated Financial Management Information System |



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix E
Office of Audits Major Contributors to This Report

Kristen Bernard, Division Director
Christopher Browning, Audit Manager
Swati Nijhawan, Senior Program Analyst
Michael Thorgersen, Program Analyst
Morgan Wade, Program Analyst
Kathy Hughes, Referencer



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix F
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
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
Acting Administrator, Federal Emergency Management Agency
Federal Emergency Management Agency Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

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