OFFICE OF INSPECTOR GENERAL

Testimony of Senior Official Performing the Duties of the Inspector General John V. Kelly

Before the Committee on Homeland Security

Subcommittee on Emergency Preparedness, Response, and Communications

U.S. House of Representatives

"Using Innovative Technology and Practices to Enhance the Culture of Preparedness"

Homeland Security

July 25, 2018
2:00 PM

Chairman Donovan, Ranking Member Payne, and Members of the subcommittee, thank you for inviting me here today to discuss information technology (IT) and management practices at the Federal Emergency Management Agency (FEMA). My testimony today will focus on the Department of Homeland Security (DHS) Office of Inspector General's (OIG) work to assess the efficiency and effectiveness of FEMA's IT in supporting mission operations.

Numerous OIG audits conducted since 2005 have disclosed that FEMA's outdated IT systems and infrastructure did not enable FEMA personnel to effectively carry out disaster response and recovery efforts. Significant longstanding deficiencies continue to hamper emergency support operations in the following areas:

- Inability to integrate FEMA's internal systems to perform end-to-end mission functions;
- Inability to track and manage disaster-related funds effectively;
- Inability to share information with external emergency management partners; and
- Limited real-time awareness or coordination across disaster response efforts.

We attribute these deficiencies to ineffective FEMA IT management practices. Principally, FEMA lacks key elements needed to carry out centralized planning, development, and management of agency-wide IT, including:

- A comprehensive IT strategic plan with clearly defined goals and objectives to guide program office initiatives;
- A modernization approach to modernize its IT infrastructure and systems;
- Comprehensive understanding of existing IT resources and needs throughout FEMA;
- Centralized budget authority for the FEMA Chief Information Officer (CIO) to provide guidance and oversight; and
- An established, formal governance process to guide agency-wide IT decisions.

These challenges have resulted in considerable wasted resources as system users conducted time-consuming, manual workarounds and ad-hoc processes. Such inefficiencies caused delays and prevented FEMA from being able to

quickly scale up and sustain the increased workloads and information sharing required to respond to major disasters. Until FEMA provides the IT systems and capabilities needed to meet the demands posed by emergency management, timely response and recovery from disasters will be hindered, increasing the risk of delays in providing disaster assistance and grants.

Background

FEMA is the Federal coordinator to prepare for, prevent, respond to, and recover from domestic disasters and emergencies. FEMA is responsible for saving lives, protecting property, and protecting public health and safety in a natural disaster, act of terrorism, or other manmade disaster. To support its mission, FEMA had a budget of approximately $15.5 billion for fiscal year (FY) 2018. This represented 22% of DHS's overall budget of more than $70 billion.

Within FEMA, the Office of the Chief Information Officer (OCIO) is responsible for providing the critical IT infrastructure and systems to support the agency's response and recovery missions. FEMA has over 90 operational systems used to provide support across multiple programs. For example, FEMA personnel rely on the following mission-critical systems to accomplish its mission:

- Logistics management systems such as the Logistics Supply Chain Management System (LSCMS) and the Logistics Information Management System (LIMS III);
- Response and recovery systems such as the National Emergency Management Information System (NEMIS), the Emergency Management Mission Integrated Environment (EMMIE), and the Web-based Emergency Operations Center (WebEOC);
- Mitigation and preparedness systems such as the Non-Disaster Grants Management System (ND-Grants) and Mitigation Electronic Grants (eGrants); and
- Mission support systems such as the Web Integrated Financial Management Information System (WebIFMIS).

Despite the crucial role of technology, FEMA's IT systems historically have not fully met mission needs. Major disasters over the past number of years exposed numerous limitations in FEMA's IT infrastructure and system capabilities. We have conducted a series of audits from September 2005 to the present addressing FEMA's use of IT to support its mission operations.

Longstanding IT Deficiencies Impede FEMA Mission Operations

Despite the importance of IT for FEMA's mission, we have identified numerous problems with FEMA's IT systems and infrastructure. As early as September

2005, we reported that system improvements and additional IT user support were needed to better support response and recovery operations.[1] In December 2006, we identified significant challenges to FEMA establishing strategic IT direction and defining the requirements for system modernization.[2] Further, in May 2008, we reported that FEMA's logistics information management systems did not provide complete asset visibility of disaster goods, such as commodities and property, from initial shipment to final distribution in disaster areas.[3]

System Integration Issues

More recently, our 2011 and 2015 audit reports on FEMA's IT disclosed that FEMA's outdated mission-critical systems could not fully support emergency mission operations.[4] The audits concluded a lack of integration among FEMA's IT systems was impeding a number of FEMA's essential operational functions, including logistics management, asset management, and financial management. Examples of the lack of integration among the various types of systems include:

- **Logistics Management Systems**: FEMA's multiple logistics systems were not integrated and could not support its end-to-end supply chain process. FEMA had not integrated the systems used in its property inventory and supply chain processes, which resulted in fragmentation of data across multiple logistics systems. Specifically, the property management system, LIMS III, and the supply chain management system, LSCMS, were not integrated. Most commodities, such as IT equipment and furniture, were tracked in both systems, with staff performing the same functions in each system. Also, the information in LIMS III was not timely or accurate because data was not automatically shared between LIMS III and LSCMS as commodities were shipped. Given this, users had to manually enter data in LIMS III to close out orders. Moreover, because the shipment did not show up in LIMS III until FEMA personnel received the shipment, personnel manually updated LIMS III as shipments were received. Consequently, the processes for shipping and receiving was labor-intensive and redundant.

  As mandated by Congress in 2005, FEMA developed LSCMS to enable a timely and effective response to disasters and real-time visibility over

[1] *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery* (OIG-05-36).
[2] *FEMA's Progress in Addressing Information Technology Management Weaknesses* (OIG-07-17).
[3] *Logistics Information Systems Need to Be Strengthened at the Federal Emergency Management Agency* (OIG-08-60).
[4] *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology* (OIG-11-69); and *FEMA Faces Challenges in Managing Information Technology* (OIG-16-10).

shipments of emergency supplies.[5] We reported in 2014 that FEMA's supply chain management system may not be effective during a catastrophic disaster. We found that FEMA did not properly plan and document acquisition requirements and may not ever meet critical performance requirements, which can impair its ability to efficiently and effectively aid survivors of catastrophic disasters. Our 2014 report contained 11 recommendations, two of which remain open.[6]

- **Personnel and Property Management Systems:** FEMA had not integrated systems to support personnel and property management functions needed to assign IT equipment at disaster sites. As we initially reported in 2005, FEMA's personnel deployment system and its property management system, LIMS III, did not support effective or efficient coordination of deployment operations.[7] Given the continuation of this issue, FEMA employees completed a number of steps to manually check in and obtain property, such as IT equipment, at a disaster site. We concluded that until an effective link between the personnel and property management systems was established, FEMA faced additional work due to inefficient management of property and personnel.

- **Financial and Acquisition Management Systems:** FEMA's ability to track and manage disaster-related funds was hindered by the fact that the financial system and the acquisitions system were not integrated. Combined, these systems handled 80% of budget disaster funds. However, each system operated on a different technical platform, with financial data updates sent to each system at different times. As a result, the two systems were operating without synchronized data, and field office employees manually tracked and reconciled funds that were allocated across different disaster activities. Additionally, manual steps were required to deobligate excess funds after requisitions were completed. Although this step should be done automatically, personnel performed manual deobligations that totaled $21 million for FY 2010 disaster funds.

- **Grants Management Systems:** A lack of integration was most notable in FEMA's nine different systems used to support the agency's grant programs, each developed independently to support a specific type of grant. These systems did not enable Grant Managers to monitor FEMA activity across grant programs, as managers had to access one system at

[5] *FEMA's Logistics Supply Chain Management System May Not Be Effective During a Catastrophic Disaster,* (OIG-14-151).
[6] Additionally, we have an ongoing review examining to what extent FEMA managed and distributed commodities in the Commonwealth of Puerto Rico in response to Hurricanes Maria and Irma.
[7] *Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery* (OIG-05-36).

a time to search for open grants and compile the results. One region created its own tool for tracking information across FEMA's various grant systems. The numerous unintegrated grant systems also created complexity for grant recipients, such as states, who need to access multiple systems to process grant awards and request payment.

- **Grants/Financial Management Systems Interface:** FEMA personnel were also unable to detect duplicate grant submissions, due to the lack of integration between the grant systems and the agency's main financial system, WebIFMIS. FEMA personnel manually entered information from the grant system into WebIFMIS at certain stages in the grant process. Similarly, the preparedness grant system, ND-Grants, did not fully interface with WebIFMIS, resulting in the need to manually enter information to complete and close out a grant in both ND-Grants and WebIFMIS. Given these limitations, according to regional staff, if a state were to suffer multiple disasters, one person could apply for assistance for each of the different disasters and not be identified. Further, the inability of enterprise systems to accurately transmit grant information between certain systems can result in grantees receiving incorrect notices that they are not in compliance with grant requirements, which has resulted in delays in making grant funds available.

- **Collaboration Systems:** FEMA's primary watch and response collaboration system, WebEOC, was not integrated with agency systems used to request immediate short-term emergency response assistance. Instead, FEMA personnel entered information into WebEOC, which processes and tracks the mission assignment requests, and entered the same information into the financial approval system used to process mission assignments, and WebIFMIS. Likewise, the FEMA WebEOC was not integrated with the WebEOC used by state emergency operation centers, resulting in an inefficient manual process to update WebEOC with information from the state centers about ongoing disasters. Specifically, a region had to send FEMA staff to a state emergency operation center to review the state's information. If a state's request for assistance was submitted in the state system, a FEMA staff member printed it out and manually entered the same data into the FEMA WebEOC.

Lack of Required Systems Functionality

The lack of system integration as well as other system deficiencies resulted in personnel engaging in inefficient, time-consuming business practices on a daily basis. For example:

- One region created 30 Excel spreadsheets to have the information needed to report on disaster spending by states in response to congressional

requests. In addition, field personnel created their own tools, such as spreadsheets and databases, to fill the gaps from enterprise system limitations.

- FEMA personnel could not simply retrieve a standard report from NEMIS that contained a grant applicant's entire record. Instead, grant personnel accessed numerous different screens in NEMIS and compile the results.

- Reports in EMMIE could only be prepared for one disaster at a time. To obtain information across several disasters, personnel accessed and retrieved a report for each individual disaster and manually combined the data into one report. In addition, one grant specialist said that none of FEMA's non-disaster grants systems were able to generate reports listing open, closed, or expired grants collectively.

- FEMA did not have an electronic capability for the states, its foremost external partners, to use when requesting assistance during disasters. Instead, to request Federal assistance from FEMA, states used a paper Action Request Form. After the form was faxed, FEMA personnel entered request information into a tracking system that was intended to track the request through disposition.

- Although NEMIS eGrants was supposed to be an electronic system of records, it did not have a closeout module. Without a closeout capability, FEMA personnel relied on paper forms and manual data entry to finalize grants in the system.

- Officials in FEMA's Mitigation Directorate said they relied on a paper-based application process for the Hazard Mitigation Grant Program. As a result, according to FEMA's Mitigation office, an average of 100 to 200 paper applications received during each disaster, had to be manually entered into the system.

IT Deficiencies Attributable to FEMA IT Management Challenges

We attributed FEMA's longstanding system deficiencies to numerous challenges involving insufficient IT planning and governance agency-wide.

- **Planning**: In 2011, we reported that FEMA had not performed the necessary planning activities to guide its IT modernization efforts.[8] As a result of our follow-up audit in 2015, we reported that FEMA had developed numerous IT planning documents but had not yet executed

[8] *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology* (OIG-11-69).

them, in part because of the frequent turnover in the CIO position within the agency. FEMA had six different individuals, either appointed or acting, serving in the CIO position over the previous 10 years. For this time period, the average tenure of the FEMA CIO was about 15 months. Without a comprehensive, agency-wide IT strategic plan, the OCIO lacked a clear end-state vision to coordinate and prioritize modernization initiatives across program offices.

Without such a plan, the OCIO and its customers focused on immediate needs, rather than addressing the long-term modernization efforts necessary to improve outdated, legacy IT infrastructure and systems.

- **Architecture:** FEMA had not completed its efforts to develop a complete agency-wide architecture that can be used for decision-making to guide and constrain investments and to provide a blueprint for IT modernization. Without a comprehensive baseline architecture, the OCIO was hindered in guiding IT investments toward a standardized and integrated environment. The OCIO had not yet completed the baseline architecture due to staffing and funding shortages.

- **Systems Inventory**: The FEMA OCIO did not have an understanding of existing IT resources and needs throughout FEMA. Specifically, FEMA did not have a complete inventory of its systems to support disasters. Instead, numerous separate inventories were maintained throughout the agency and were not shared. OCIO personnel estimated that the number of FEMA's systems across all regional offices ranges from 90 to as high as 700.

- **Decentralized IT Funding:** The manner in which IT programs receive direct funding for operations each year contributed to decentralized IT development practices. Specifically, FEMA program and field offices developed IT systems independent of the OCIO without oversight or guidance. Developing new systems on the network without OCIO involvement created concerns as to whether systems would operate effectively, meet security standards, or contain redundant IT functionality already in place. For example, one directorate spent approximately $7.5 million developing an IT system which was ultimately unable to meet FEMA's security requirements. Although the OCIO had developed a standard systems life cycle practice to be used for all IT projects, the process has not yet been institutionalized throughout FEMA.

  The decentralization of IT funds and development also has been a major obstacle to effective management of FEMA's IT environment. During FY 2010, FEMA spent $391 million for agency-wide IT needs; however, OCIO's spending of $113 million accounted for only 29% of that total IT

spending. The program offices spent the remaining $278 million, comprising the majority of the agency's IT-related spending. In FY 2018, OCIO spending was $164 million, comprising 40% of the agency's total IT budget of $396 million.

Efforts to modernize and integrate the agency's critical mission support systems had been put on hold due to department-wide consolidation plans, and lack of funding. For example, FEMA was not able to plan or fund asset management or financial systems upgrades while DHS officials were identifying a department-wide asset management solution. Also, funding for critical enhancements and upgrades to logistics management systems and financial systems had decreased over the preceding years. FEMA was also hamstrung by the increasing costs of software upgrades for its 20-year-old technologies.

- **Agency-wide IT Governance:** FEMA struggled to implement effective agency-wide IT governance. FEMA instituted an IT Governance Board (ITGB) in February 2012; however, the board's functioning proved ineffective and it eventually stopped holding meetings. In addition, ITGB struggled to make decisions on FEMA-wide IT initiatives. For example, the *Consolidated Appropriations Act, 2012,* allocated $13.662 million for FEMA to modernize IT systems.[9] One of the main initiatives undertaken by the ITGB was to decide which projects should receive this funding. However, the process ITGB implemented to solicit, evaluate, and select candidate IT projects was unsuccessful. ITGB did not use the results obtained from this process because members did not concur with the scoring results.

- **CIO Authority:** FEMA had not implemented effective agency-wide IT governance, in part, because the CIO still did not have sufficient authority to effectively lead the agency's decentralized IT environment. As we reported in 2011, the OCIO's budget still accounted for only one-third of the agency's total IT spending, with the FEMA program offices accounting for the remaining two thirds. As previously stated, the OCIO's FY 2014 IT spending was approximately $170 million of $450 million for the entire agency.

Recommendations

To address the IT system and management issues identified in our 2011 reports, we made a number of recommendations to the Chief Information Officer in the following areas:

- Develop a comprehensive IT strategic plan,

[9] Public Law 112–74.

- Complete and implement a FEMA enterprise architecture,
- Establish a comprehensive IT systems inventory,
- Establish an agency-wide IT budget planning process and obtain agency-wide IT investment review authority, and
- Establish a consolidated modernization approach for FEMA's mission-critical IT systems.

We closed these 2011 recommendations based on FEMA's quarterly reports to us on corrective actions taken.

Further, in 2015, we recommended the FEMA CIO finalize key planning documents related to IT modernization and execute against those planning documents, fully implement an IT governance board, improve integration and functionality of existing systems, and implement agency-wide acquisition, development, and operation and maintenance standards. Of the five recommendations from the 2015 report, four remain open. We closed one recommendation regarding implementing an IT governance board based on documentation that FEMA provided.

Follow-on Audits to Determine Progress in FEMA's IT Management

As we periodically do, we conducted a verification review in December 2017 to assess FEMA's efforts to address our 2015 report recommendations. Congressional interest, as well as our analysis of the compliance updates, indicated a need for further review to determine the adequacy of FEMA's efforts to resolve our open recommendations. Since the publication of our report in 2015, FEMA has provided six compliance updates on its efforts to address our five report recommendations.

However, we found during our January and February 2018 review fieldwork that FEMA had made limited progress in improving its IT management and had not taken steps to adequately address our recommendations. Many of the issues we reported based on our prior audits dating back to 2005 remained unchanged, adversely impacting day-to-day operations and mission readiness. Especially disconcerting, our recent work revealed that the justification that FEMA provided to support our closing the recommendation to implement an IT governance board was misleading and FEMA had not truly met the intent of the recommendation.

Given these deficiencies, we suspended our verification review and issued a Management Alert.[10] The Management Alert indicated that, given competing priorities, the CIO had removed the funding and staff resources needed to effectively address our report recommendations. The Management Alert also

[10] *Management Alert-Inadequate Progress in Addressing Open Recommendations from our 2015 Report, "FEMA Faces Challenges in Managing Information Technology,"* (OIG-18-54).

stated we would initiate a more comprehensive audit regarding FEMA's IT management approach, with the objectives of assessing the extent to which FEMA has implemented IT management practices mandated for Federal agencies, and identifying challenges to ensuring FEMA's IT systems adequately support disaster response mission operations. We began our current audit work in May 2018.

As part of our ongoing audit, we seek to identify and assess any challenges, impediments, or constraints associated with the ability of FEMA's IT systems to adequately support day-to-day mission operations. We are assessing FEMA's approaches and outcomes related to key IT management practices, including IT strategic planning, governance, budgeting, and acquisitions. Lastly, we are following up on specific issues identified in our previous reports on FEMA's IT management. To date, the audit team has conducted numerous interviews with FEMA personnel across all program offices. The team has also traveled to FEMA's field offices in Houston, TX and Austin, TX to learn about specific IT-related challenges that FEMA personnel experienced during their response and recovery efforts for Hurricane Harvey. We expect to issue our final audit report early in 2019.

Conclusion

IT systems play a vital role in supporting FEMA' response and recovery efforts. Slow progress in addressing longstanding IT issues can hamper disaster response efforts and result in wasted money, continued ineffective systems, and inefficient processing. Having reliable and efficient IT systems and infrastructure is critical to support disasters that typically occur from year-to-year, as well as the increased disaster relief efforts in the wake of the 2017 hurricane season. To date, Congress has appropriated about $49.5 billion to FEMA's Disaster Relief Fund for these recovery efforts.

Strong IT leadership direction is needed to stop this pattern and ensure corrective actions to overcome the IT management challenges once and for all. Improvement is essential -- for the sake of the taxpayer, FEMA IT users, first responders, and disaster victims. Our ongoing audit is aimed at emphasizing this need for positive change. We will advise you on the results of our ongoing work once completed.

Mr. Chairman, this concludes my testimony. I am happy to answer any questions you or other members of the Subcommittee may have.