April 2016

INFORMATION TECHNOLOGY

FEMA Needs to Address Management Weaknesses to Improve Its Systems

GAO Highlights

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

Why GAO Did This Study

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

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

What GAO Recommends

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

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

What GAO Found

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

- **Governance and oversight:** FEMA established an investment review board to select and oversee IT investments, as called for by leading practices. But the board has not fully defined roles and responsibilities of key members, working groups, and individuals, and it does not have clearly defined procedures for selecting and overseeing investments. As a result, the agency lacks adequate visibility into and oversight of IT investment decisions and activities.

- **IT modernization:** FEMA has begun to take steps to modernize its IT environment, but key planning documents are not current and complete. For example, the agency has an IT strategic plan and is currently drafting its modernization plan; however, the plans do not reflect the agency's current goals and objectives. Further, the IT strategic plan describes the Chief Information Officer's (CIO) mission, goals, and objectives through fiscal year 2016, but has not been updated since 2013. In addition, while the Office of the CIO is currently drafting the agency's IT modernization plan, including an implementation strategy and an overall schedule, it is not yet final. As a result, the agency is limited in its ability to move toward its goal to modernize its systems and eliminate duplicative IT investments.

- **Workforce planning:** The agency has not yet established time frames to address long-standing workforce management challenges. For example, while it conducted a workforce assessment to identify skill levels of employees in the agency's Office of the CIO, it has not completed recommended actions called for by this assessment. In addition, its workforce planning efforts have not included an assessment of the many IT staff located in the agency's regions and other offices. Consequently, FEMA has less assurance that its IT workforce will have the skills needed to successfully manage its programs.

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