April 2019

FEMA GRANTS MODERNIZATION

Improvements Needed to Strengthen Program Management and Cybersecurity

GAO Highlights

Highlights of GAO-19-164, a report to the Chairman of the Subcommittee on Emergency Preparedness, Response, and Recovery, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

FEMA, a component of DHS, annually awards billions of dollars in grants to help communities prepare for, mitigate the effects of, and recover from major disasters. However, FEMA's complex IT environment supporting grants management consists of many disparate systems. In 2008, the agency attempted to modernize these systems but experienced significant challenges. In 2015, FEMA initiated a new endeavor (the GMM program) aimed at streamlining and modernizing the grants management IT environment.

GAO was asked to review the GMM program. GAO's objectives were to (1) determine the extent to which FEMA is implementing leading practices for reengineering its grants management processes and incorporating needs into IT requirements; (2) assess the reliability of the program's estimated costs and schedule; and (3) determine the extent to which FEMA is addressing key cybersecurity practices. GAO compared program documentation to leading practices for process reengineering and requirements management, cost and schedule estimation, and cybersecurity risk management, as established by the Software Engineering Institute, National Institute of Standards and Technology, and GAO.

What GAO Recommends

GAO is making eight recommendations to FEMA to implement leading practices related to reengineering processes, managing requirements, scheduling, and implementing cybersecurity. DHS concurred with all recommendations and provided estimated dates for implementing each of them.

View GAO-19-164. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

Of six important leading practices for effective business process reengineering and information technology (IT) requirements management, the Federal Emergency Management Agency (FEMA) fully implemented four and partially implemented two for the Grants Management Modernization (GMM) program (see table). Specifically, FEMA ensured senior leadership commitment, took steps to assess its business environment and performance goals, took recent actions to track progress in delivering IT requirements, and incorporated input from end user stakeholders. However, FEMA has not yet fully established plans for implementing new business processes or established complete traceability of IT requirements.

Extent to Which the Federal Emergency Management Agency Implemented Selected Leading Practices for Business Process Reengineering and Information Technology (IT) Requirements Management for the Grants Management Modernization Program

Leading practice	Overall area rating
Ensure executive leadership support for process reengineering	●
Assess the current and target business environment and business performance goals	●
Establish plans for implementing new business processes	◑
Establish clear, prioritized, and traceable IT requirements	◑
Track progress in delivering IT requirements	●
Incorporate input from end user stakeholders	●

Legend: ●=Fully implemented, ◑=Partially implemented, ○=Not implemented.

Source: GAO analysis of Federal Emergency Management Agency documentation. | GAO-19-164

Until FEMA fully implements the remaining two practices, it risks delivering an IT solution that does not fully modernize FEMA's grants management systems.

While GMM's initial May 2017 cost estimate of about $251 million was generally consistent with leading practices for a reliable, high-quality estimate, it no longer reflects current assumptions about the program. FEMA officials stated in December 2018 that they had completed a revised cost estimate, but it was undergoing departmental approval. GMM's program schedule was inconsistent with leading practices; of particular concern was that the program's final delivery date of September 2020 was not informed by a realistic assessment of GMM development activities, and rather was determined by imposing an unsubstantiated delivery date. Developing sound cost and schedule estimates is necessary to ensure that FEMA has a clear understanding of program risks.

Of five key cybersecurity practices, FEMA fully addressed three and partially addressed two for GMM. Specifically, it categorized GMM's system based on security risk, selected and implemented security controls, and monitored security controls on an ongoing basis. However, the program had not initially established corrective action plans for 13 medium- and low-risk vulnerabilities. This conflicts with the Department of Homeland Security's (DHS) guidance that specifies that corrective action plans must be developed for every weakness identified. Until FEMA, among other things, ensures that the program consistently follows the department's guidance on preparing corrective action plans for all security vulnerabilities, GMM's system will remain at increased risk of exploits.