United States Government Accountability Office

Report to the Chairman of the Subcommittee on Emergency Preparedness, Response, and Recovery, Committee on Homeland Security, House of Representatives

April 2019

FEMA GRANTS MODERNIZATION

Improvements Needed to Strengthen Program Management and Cybersecurity

Accessible Version

GAO-19-164

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	Fully implemented
Assess the current and target business environment and business performance goals	Fully implemented
Establish plans for implementing new business processes	Partially implemented
Establish clear, prioritized, and traceable IT requirements	Partially implemented
Track progress in delivering IT requirements	Fully implemented
Incorporate input from end user stakeholders	Fully 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.

Contents

Tables

Figures

Abbreviations

AFG	Assistance to Firefighters Grants
DHS	Department of Homeland Security
EMMIE	Emergency Management Mission Integrated Environment
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Modernization Act of 2014 and Federal Information Security Management Act of 2002
GMM	Grants Management Modernization
IT	information technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

April 9, 2019

The Honorable Donald M. Payne, Jr.
Chairman
Subcommittee on Emergency Preparedness, Response, and Recovery
Committee on Homeland Security
House of Representatives

Dear Mr. Chairman:

The Federal Emergency Management Agency (FEMA), a component of the Department of Homeland Security (DHS), leads the federal effort to mitigate, respond to, and recover from disasters. FEMA is responsible for saving lives and protecting property, public health, and safety in a natural disaster, act of terrorism, or other manmade disaster.

FEMA accomplishes a large part of its mission through awarding grants to state, local, and tribal governments and nongovernmental entities to help communities prevent, prepare for, protect against, mitigate the effects of, respond to, and recover from disasters and terrorist attacks. According to the agency, these grants represent about 70 percent of its annual budget—FEMA's annual budget averaged about $15 billion per year for the past 3 fiscal years (2016, 2017, and 2018).

The federal government, including FEMA, obligates billions of dollars in grants each year for disaster assistance, and the increases in the number and severity of disasters has become a key source of federal fiscal exposure.[1] We reported in September 2016 that the federal government had obligated at least $277.6 billion in disaster assistance grants during fiscal years 2005 through 2014. Of this amount, FEMA had obligated about $104.5 billion in disaster assistance grants.[2]

[1]The term fiscal exposure refers to the responsibilities, programs, and activities that may either legally commit the federal government to future spending or create the expectation for future spending. See GAO, *Fiscal Exposures: Improving Cost Recognition in the Federal Budget*, GAO-14-28 (Washington, D.C.: Oct. 29, 2013). Also, see GAO's Federal Fiscal Outlook web page: http://www.gao.gov/americas_fiscal_future.

[2]GAO, *Federal Disaster Assistance: Federal Departments and Agencies Obligated at Least $277.6 Billion during Fiscal Years 2005 through 2014,* GAO-16-797 (Washington, D.C.: Sept. 22, 2016).

FEMA relies heavily on the use of information technology (IT) to support its grant award processes. According to its IT investment portfolio for fiscal year 2018, the agency reported spending about $405 million on these investments.

However, the agency has long reported that its grants management IT environment is highly complex and consists of many disparate systems and labor-intensive manual processes. This has led to poor information sharing and reporting capabilities, difficulties in reconciling financial data, and an increased burden on grant recipients.

In 2008, FEMA attempted to develop and implement a single grants processing solution, referred to as the Emergency Management Mission Integrated Environment (EMMIE), to address these IT concerns and modernize its legacy grants management systems. However, as we have previously reported, the program experienced significant implementation challenges, which resulted in a solution that was missing important capabilities.[3] Subsequently, in 2015, FEMA initiated a new endeavor to modernize and streamline the agency's grants management IT environment. This most recent initiative is referred to as the Grants Management Modernization (GMM) program.

Given the importance of having modernized grants management systems and FEMA's past system implementation challenges, you asked us to review the GMM program. Our specific objectives were to (1) determine the extent to which FEMA is implementing leading practices for reengineering its grants management business processes and incorporating business needs into IT requirements for GMM; (2) assess the reliability of the GMM program's estimated costs and schedule; and (3) determine the extent to which FEMA is addressing key cybersecurity practices for GMM.

To address the first objective, we reviewed leading practices and guidance that GAO and the Software Engineering Institute have

[3]GAO, *Information Technology: FEMA Needs to Address Management Weaknesses to Improve Its Systems,* GAO-16-306 (Washington, D.C.: Apr. 5, 2016) and *Disaster Assistance: Opportunities to Enhance Implementation of the Redesigned Public Assistance Grant Program,* GAO-18-30 (Washington, D.C.: Nov. 8, 2017).

developed,[4] and from these sources, identified six practice areas associated with business process reengineering and IT requirements management. These selected areas, in our professional judgment, represented foundational practices that were of particular importance to the successful implementation of an IT modernization effort that is using incremental software development processes.

We then reviewed relevant GMM program documentation, such as grants management business processes, the acquisition program baseline, IT requirements documents, and a concept of operations. We assessed the program documentation against the six selected practice areas and made determinations on the extent to which the agency had

- fully implemented the practice area (FEMA provided complete evidence showing that it fully implemented the practice area);
- partially implemented the practice area (FEMA provided evidence showing that it partially implemented the practice area); or
- not implemented the practice area (FEMA did not provide evidence showing that it implemented any of the practice area).

We also observed the program's incremental software development activities and a demonstration of the program's automated requirements management tool at GMM facilities in Washington, D.C. Further, we interviewed FEMA officials regarding their efforts to streamline grants management business processes, collect and incorporate stakeholder input, and manage GMM's IT requirements.

To assess the reliability of data from the program's automated IT requirements management tool, we interviewed knowledgeable officials about the quality control procedures used by the program to ensure accuracy and completeness of the data. In addition, we assessed the data against other relevant program documentation on GMM's requirements. We determined that the data used were sufficiently reliable

[4]GAO, *Business Process Reengineering Assessment Guide*, Version 3, GAO/AIMD-10.1.15 (Washington, D.C.: May 1997); Software Engineering Institute, *Capability Maturity Model® Integration for Development*, Version 1.3 (Pittsburgh, Pa.: November 2010); and draft *GAO Agile Assessment Guide*, Version 6A. To develop the draft Agile guide, we have worked closely with Agile experts in the public and private sector and some chapters of the guide are considered more mature because they were reviewed by the expert panel. For our assessment, we used these chapters of the draft guide.

for the purpose of evaluating GMM's practices for managing IT requirements.

For the second objective, we reviewed documentation supporting GMM's lifecycle cost estimate and schedule. Specifically, we evaluated documentation regarding the program's May 2017 lifecycle cost estimate against the leading practices for developing a comprehensive, accurate, well-documented, and credible cost estimate identified in GAO's Cost Estimating and Assessment Guide.[5]

Additionally, we evaluated documentation regarding GMM's integrated master schedule, dated May 2018, against the leading practices for developing a comprehensive, well-constructed, credible, and controlled schedule identified in GAO's Schedule Assessment Guide.[6] We also interviewed responsible GMM program officials to understand their practices for developing and maintaining the program cost estimate and schedule. We found that the cost data were sufficiently reliable and we noted in our report the instances where the quality of the schedule data impacted the reliability of the program's schedule.

To address the third objective, we reviewed the National Institute of Standards and Technology's (NIST) risk management framework and identified key cybersecurity practices.[7] Next, we reviewed DHS's and FEMA's cybersecurity policies and guidance, as well as documentation on FEMA's authorization to operate[8] for GMM's engineering and test environment. This environment went live in February 2018 and had obtained authorization to operate at the time that we began our review.[9]

[5]GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs,* GAO-09-3SP (Washington, D.C.: March 2009).

[6]GAO, *Schedule Assessment Guide: Best Practices for Project Schedules,* GAO-16-89G (Washington, D.C.: December 2015).

[7]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

[8]According to NIST, an authorization to operate is an official management decision, made after all cybersecurity assessment activities have been performed, stating that the system is authorized for use and explicitly accepting the risk to the organization.

[9]Subsequent to the start of our review, GMM conducted a separate authorization to operate process for the GMM production environment, in July 2018.

We assessed FEMA's cybersecurity documentation against the NIST framework's five key cybersecurity practices[10] and assessed the extent to which the agency had

- fully addressed the practice area (FEMA provided complete evidence which showed that it fully implemented the practice area),
- partially addressed the practice area (FEMA provided evidence which showed that it partially implemented the practice area), or
- not addressed the practice area (FEMA did not provide evidence which showed that it implemented any of the practice area).

We also interviewed cognizant officials in the GMM program office and FEMA's Office of the Chief Information Officer (OCIO). We obtained information from these officials about their efforts to assess, document, and review cybersecurity controls for GMM.

To assess the reliability of data from the program's automated security controls management tool, we interviewed knowledgeable officials about the quality control procedures used by the program to assure accuracy and completeness of the data. We also compared the data to other relevant program documentation on GMM security controls for the engineering and test environment. We found that some of the security controls data we examined were sufficiently reliable for the purpose of evaluating FEMA's cybersecurity practices for GMM, and we noted in our report the instances where the accuracy of the data impacted the program's ability to address key cybersecurity practices. Additional details on our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from December 2017 to April 2019 in accordance with 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[10]The framework identifies six total practices, but for reporting purposes we combined two interrelated practices into one practice, thus resulting in five key cybersecurity practices.

Background

FEMA's mission is to help people before, during, and after disasters. It provides assistance to those affected by emergencies and disasters by supplying immediate needs (e.g., ice, water, food, and temporary housing) and providing financial assistance grants for damage to personal or public property. FEMA also provides non-disaster assistance grants to improve the nation's preparedness, readiness, and resilience to all hazards.

FEMA accomplishes a large part of its mission through awarding grants to state, local, and tribal governments and nongovernmental entities to help communities prevent, prepare for, protect against, mitigate the effects of, respond to, and recover from disasters and terrorist attacks. As previously mentioned, for fiscal years 2005 through 2014, the agency obligated about $104.5 billion in disaster relief grants.[11] In addition, as of April 2018, the four major disasters in 2017—hurricanes Harvey, Irma, and Maria; and the California wildfires—had resulted in over $22 billion in FEMA grants.[12]

Overview of FEMA's Grants Management Programs and Administration

The current FEMA grants management environment is highly complex with many stakeholders, IT systems, and users. Specifically, this environment is comprised of 45 active disaster and non-disaster grant programs, which are grouped into 12 distinct grant categories.[13]

[11]GAO-16-797.

[12]GAO, *2017 Hurricanes and Wildfires: Initial Observations on the Federal Response and Key Recovery Challenges,* GAO-18-472 (Washington, D.C.: Sept. 4, 2018). The $22 billion in obligated FEMA grants for the four major disasters in 2017 are in addition to the $104.5 billion that FEMA obligated for disaster assistance during fiscal years 2005 through 2014.

[13]The number of active grant programs varies based on programs being authorized or discontinued and how "grant programs" are defined. In 2018, FEMA Office of Chief Counsel officials identified 37 programs, whereas GMM program officials identified 45 programs because they defined "grant programs" more broadly and further decomposed the programs to facilitate the development of the GMM solution. For this report, we use GMM's 45 grant programs (listed in appendix II).

For example, one program in the Preparedness: Fire category is the Assistance to Firefighters Grants (AFG) program, which provides grants to fire departments, nonaffiliated emergency medical service organizations, and state fire training academies to support firefighting and emergency response needs. As another example, the Housing Assistance grant program is in the Recovery Assistance for Individuals category and provides financial assistance to individuals and households in geographical areas that have been declared an emergency or major disaster by the President.

Table 1 lists FEMA's non-disaster and disaster-based grant categories.

Table 1: Federal Emergency Management Agency's Grant Categories

Grant category	Disaster	Non-disaster	Both
Preparedness: Fire	NA	Yes	NA
Preparedness: Chemical	NA	Yes	NA
Preparedness: Homeland Security	NA	Yes	NA
Preparedness: Standards	NA	Yes	NA
Preparedness: Training	NA	Yes	NA
Mitigation: Hazards	NA	NA	Yes
Mitigation: Community Assistance	NA	Yes	NA
Mitigation: Earthquake	NA	Yes	NA
Mitigation: Risk Management	NA	Yes	NA
Recovery (Assistance for Individuals)	Yes	NA	NA
Recovery (Assistance for Organizations/Government)	Yes	NA	NA
Response: Urban Search and Rescue	NA	NA	Yes

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

According to FEMA, the processes for managing these different types of grants vary because the grant programs were developed independently by at least 18 separate authorizing laws that were enacted over a 62-year period (from 1947 through 2009). The various laws call for different administrative and reporting requirements.

For example, the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended,[14] established the statutory authority for 11 of the grant programs, such as the administration of Public Assistance and Individual Assistance grant programs after a presidentially declared

[14]42 U.S.C. §§ 5121-5207.

disaster.[15] The act also requires the FEMA Administrator to submit an annual report to the President and Congress covering FEMA's expenditures, contributions, work, and accomplishments, pursuant to the act.[16] As another example, the National Dam Safety Program Act established one of the grant programs aimed at providing financial assistance to improve dam safety.[17]

Key stakeholders in modernizing the IT grants management environment include the internal FEMA officials that review, approve, and monitor the grants awarded, such as grant specialists, program analysts, and supervisors. FEMA has estimated that it will need to support about 5,000 simultaneous internal users of its grants management systems.

Other users include the grant recipients that apply for, receive, and submit reports on their grant awards; these are considered the external system users. These grant recipients can include individuals, states, local governments, Indian tribes, institutions of higher education, and nonprofit organizations. FEMA has estimated that there are hundreds of thousands of external users of its grants systems.

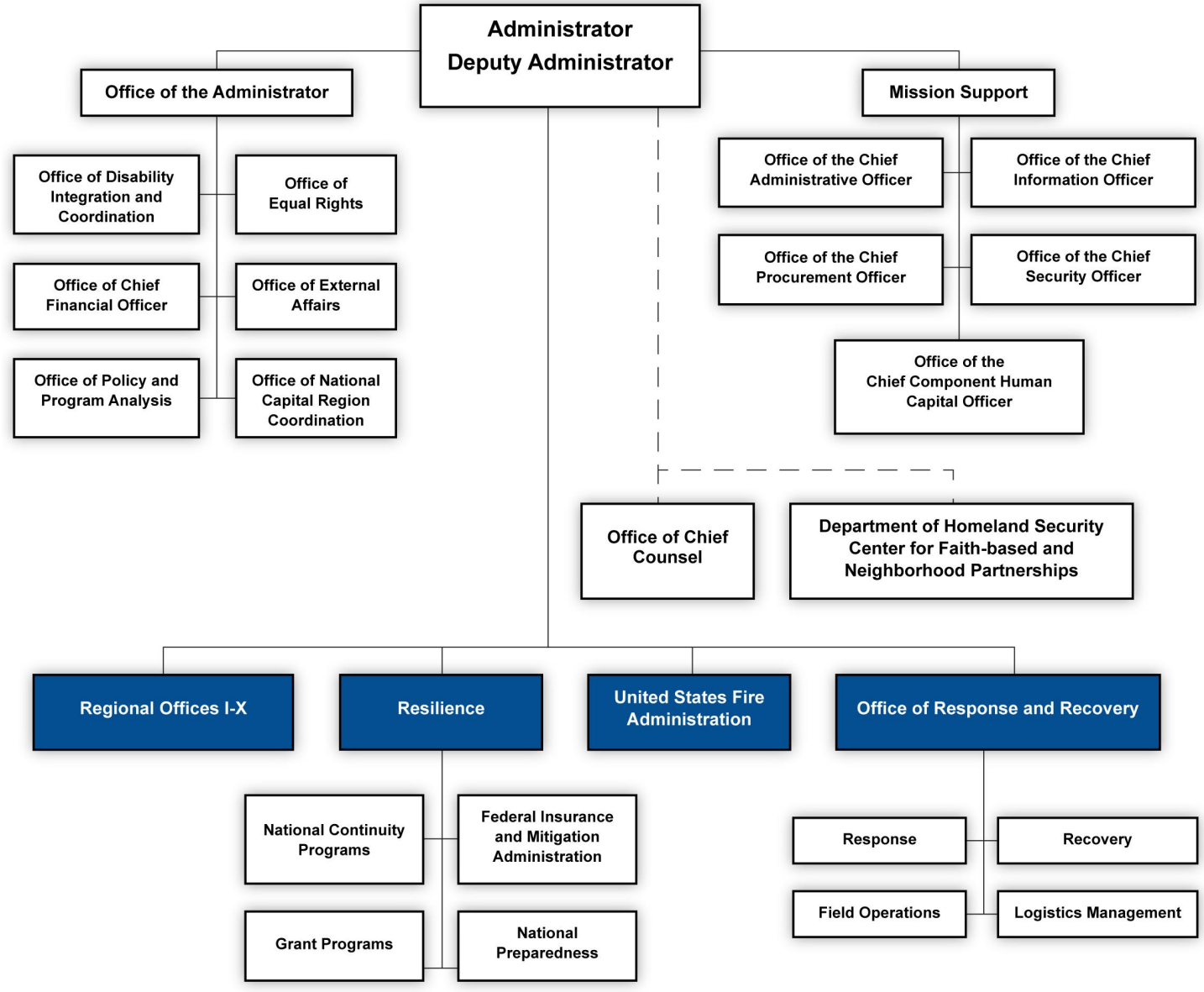
The administration of the many different grant programs is distributed across four divisions within FEMA's organizational structure. Figure 1 provides an overview of FEMA's organizational structure and the divisions that are responsible for administering grants.

[15]42 U.S.C. §§ 5170a, 5170b, 5172, 5173, 5192(a).

[16]42 U.S.C. § 5197c.

[17]33 U.S.C. § 467f.

Figure 1: Federal Emergency Management Agency's Organizational Structure and the Divisions That Are Responsible for Administering Grants



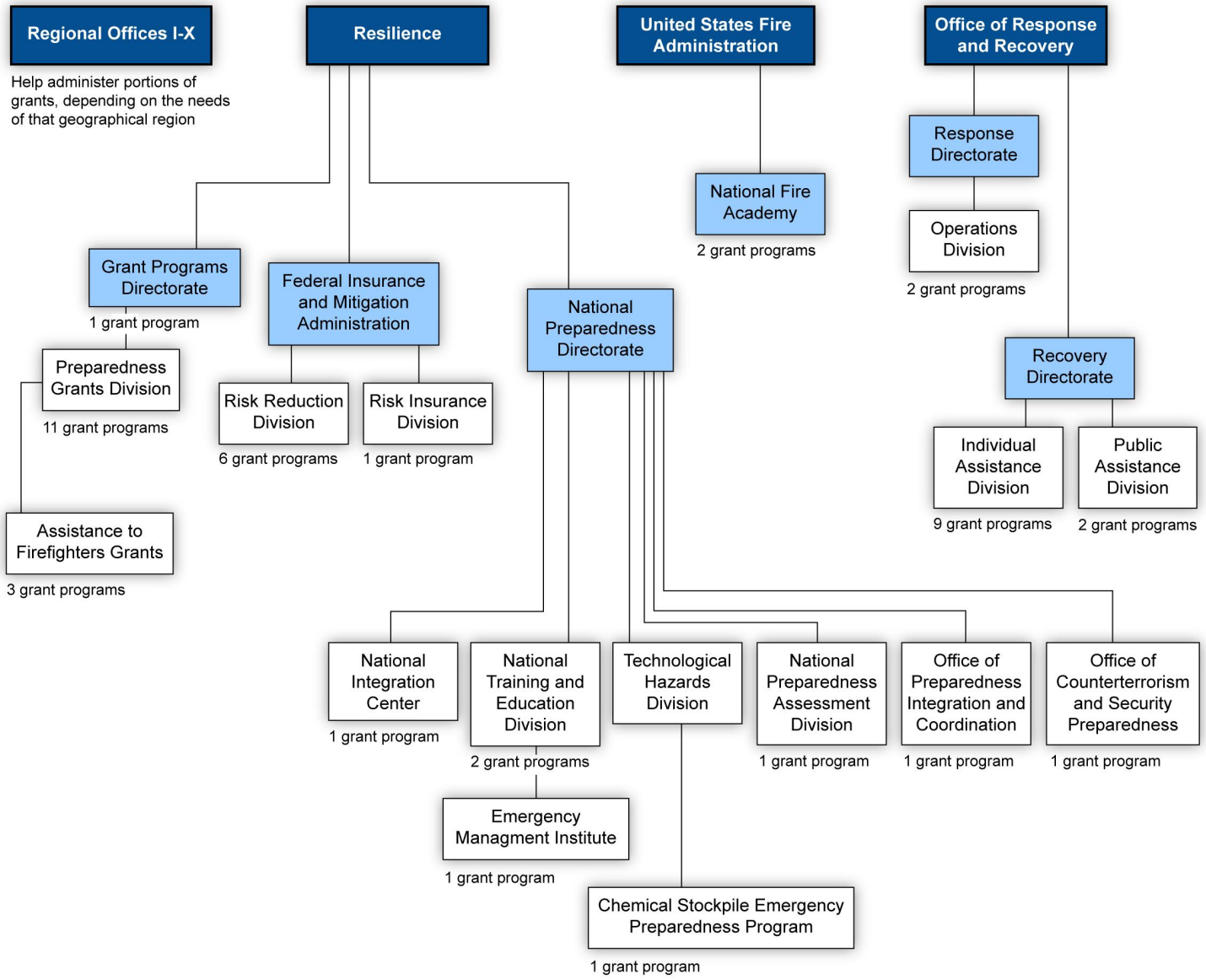
Source: GAO analysis of Federal Emergency Management Agency documentation. | GAO-19-164

Within three of the four divisions—Resilience, United States Fire Administration, and Office of Response and Recovery—16 different grant program offices are collectively responsible for administering the 45 grant

programs. The fourth division consists of 10 regional offices that help administer grants within their designated geographical regions. For example, the Office of Response and Recovery division oversees three different offices that administer 13 grant programs that are largely related to providing assistance in response to presidentially declared disasters.

Figure 2 shows the number of grant programs administered by each of the four divisions' grant program and regional offices. In addition, appendix II lists the names of the 45 grant programs.

Figure 2: Federal Emergency Management Agency's (FEMA) Structure of Grant Programs Identified by the Grants Management Modernization (GMM) Program, as of August 2018



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

Note: The number of active grant programs varies based on programs being authorized or discontinued and how "grant programs" are defined. In 2018, FEMA Office of Chief Counsel officials identified 37 programs, whereas GMM program officials identified 45 programs because they defined "grant programs" more broadly and further decomposed the programs to facilitate the development of the GMM solution.

FEMA's OCIO is responsible for developing, enhancing, and maintaining the agency's IT systems, and for increasing efficiencies and cooperation across the entire organization. However, we and the DHS Office of Inspector General (OIG) have previously reported that the grant programs and regional offices develop information systems independent of the OCIO and that this has contributed to the agency's disparate IT environment.

We and the DHS OIG have reported that this disparate IT environment was due, in part, to FEMA's decentralized IT budget and acquisition practices. For example, from fiscal years 2010 through 2015, the OCIO's budget represented about one-third of the agency's IT budget, with the grant program offices accounting for the remaining two-thirds of that budget.[18]

In February 2018, the OIG found that FEMA had shown limited progress in improving its IT management and that many of the issues reported in prior audits remained unchanged. As such, the OIG initiated a more comprehensive audit of the agency's IT management that is ongoing.[19]

Overview of FEMA's Legacy Grants Management Systems

FEMA has identified 10 primary legacy IT systems that support its grants management activities. According to the agency, most of these systems were developed to support specific grant programs or grant categories. Table 2 summarizes the 10 primary legacy systems.

[18]GAO-16-306; DHS OIG, *FEMA Faces Challenges in Managing Information Technology*, OIG-16-10 (Washington, D.C.: Nov. 20, 2015); and *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology*, OIG-11-69 (Washington, D.C.: Apr. 1, 2011).

[19]DHS OIG, *Management Alert – Inadequate FEMA Progress in Addressing Open Recommendations from our 2015 Report, "FEMA Faces Challenges in Managing Information Technology" (OIG-16-10)*, OIG-18-54 (Washington, D.C.: Feb. 26, 2018).

Table 2: Federal Emergency Management Agency's Primary Grants Management Legacy Systems

System	Description	Initial deployment of system
Assistance to Firefighters eGrant Portal	Web-based system that processes applications for the Assistance to Firefighters Grants program.	2002
Emergency Management Mission Integrated Environment (EMMIE)	Web-based system that supports the management of public assistance recovery grants throughout the entire grant lifecycle, using a standardized web-based interface.	2008
Environmental and Historic Preservation Management Information System	Web-based system that supports environmental and historic preservation reviews to ensure regulatory compliance with federal laws and Executive Orders for disaster and non-disaster grants.	2007
FEMA Applicant Case Tracker	Web-based system that was developed to supplement the EMMIE system and supports project tracking and case management functionality for pre-award activities.	2016
Grants Reporting Tool	Custom-developed web application that allows grant recipients from states, territories, and tribes to report on the allocation of their grant awards for several preparedness/homeland security grant programs.	2003
Individual Assistance	System that supports the processing of Individual Assistance grants, such as housing assistance, other needs assistance, and disaster housing operations.	1997
Mitigation eGrants	Web-based grants system that processes applications for the Flood Mitigation Assistance and Pre-Disaster Mitigation grant programs.	2003
National Emergency Management Information System – Hazard Mitigation Grant Program	Server-based application that processes mitigation grants and manages approvals on a state's mitigation plan.	1998
National Emergency Management Information System – Public Assistance	System that supports the processing of legacy public assistance grants. As of October 2018, FEMA officials stated they had mostly decommissioned the system.	1998
Non-Disaster Grants	Web-based system that supports the application, award, and administration of non-disaster-based preparedness and mitigation grants.	2011

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

According to FEMA officials, the 10 primary grant systems are all in operation (several have been for decades) and are not interoperable. As a result, individual grant programs and regional offices have independently developed work arounds intended to address existing capability gaps with the primary systems.

FEMA officials stated that while these work arounds have helped the agency partially address capability gaps with its primary systems, they are often nonstandardized processes, and introduce the potential for information security risks and errors. This environment has contributed to labor-intensive manual processes and an increased burden for grant recipients. The disparate systems have also led to poor information

sharing and reporting capabilities, as well as difficulty reconciling financial data.

The DHS OIG and we have previously highlighted challenges with FEMA's past attempts to modernize its grant management systems. For example,

- In December 2006, the DHS OIG reported that EMMIE, an effort to modernize its grants management systems and provide a single grants processing solution, was being developed without a clear understanding and definition of the future solution. The report also identified the need to ensure crosscutting participation from headquarters, regions, and states in developing and maintaining a complete, documented set of FEMA business and system requirements.[20]
- In April 2016, we found weaknesses in FEMA's development of the EMMIE system.[21] For example, we noted that the system was implemented without sufficient documentation of system requirements, an acquisition strategy, up-to-date cost estimate and schedule, total amount spent to develop the system, or a systems integration plan. In response to our findings and related recommendations, FEMA took action to address these issues. For example, the agency implemented a requirements management process that, among other things, provided guidance to programs on analyzing requirements to ensure that they are complete and verifiable.
- We reported in November 2017 that EMMIE lacked the ability to collect information on all pre-award activities and, as a result, agency officials said that they and applicants used ad hoc reports and personal tracking documents to manage and monitor the progress of grant applications. FEMA officials added that applicants often struggled to access the system and that the system was not user friendly.[22] Due to EMMIE's shortfalls, the agency had to develop another system in 2017 to supplement EMMIE with additional grant tracking and case management capabilities.

[20]DHS OIG, *FEMA's Progress in Addressing Information Technology Management Weaknesses,* OIG-07-17 (Washington, D.C.: Dec. 8, 2006).

[21]GAO-16-306.

[22]GAO-18-30.

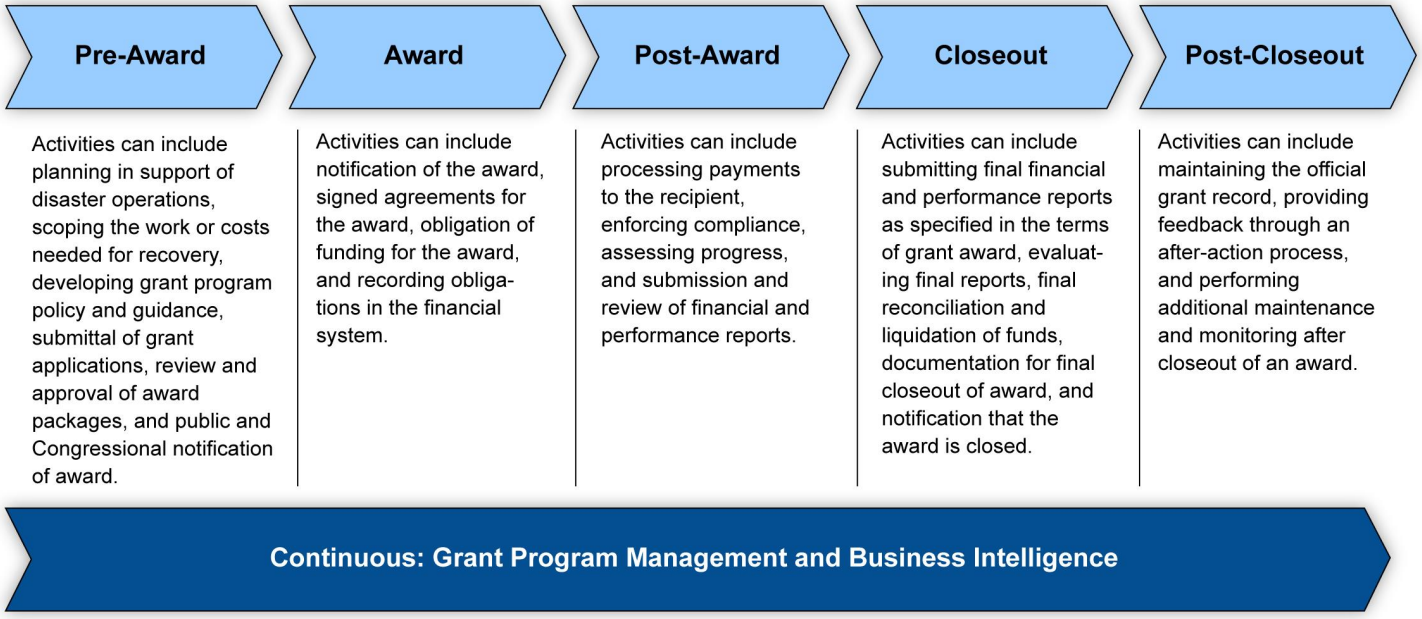
GMM Is to Address FEMA's Shortcomings with Grants Management

FEMA initiated GMM in 2015, in part, due to EMMIE's failed attempt to modernize the agency's grants management environment. The program is intended to modernize and streamline the agency's grants management environment.

To help streamline the agency's grants management processes, the program established a standard framework intended to represent a common grants management lifecycle. The framework consists of five sequential phases—pre-award, award, post-award, closeout, and post-closeout—along with a sixth phase dedicated to continuous grant program management activities, such as analyzing data and producing reports on grant awards and managing IT systems.

FEMA also established 43 distinct business functions associated with these six lifecycle phases. Figure 3 provides the general activities that may occur in each of the grant lifecycle phases, but specific activities would depend on the type of grant being administered (i.e., disaster versus non-disaster).

Figure 3: Federal Emergency Management Agency's Planned Grants Management Lifecycle



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

GMM is expected to be implemented within the complex IT environment that currently exists at FEMA. For example, the program is intended to replace the 10 legacy grants management systems, and potentially many additional subsystems, with a single IT system. Each of the 10 legacy systems was developed with its own database(s) and with no standardization of the grants management data and, according to FEMA officials, this legacy data has grown significantly over time.

Accordingly, FEMA will need to migrate, analyze, and standardize the grants management data before transitioning it to GMM. The agency awarded a contract in June 2016 to support the data migration efforts for GMM. The agency also implemented a data staging environment in October 2017 to migrate the legacy data and identify opportunities to improve the quality of the data.

Further, the GMM system is expected to interface with a total of 38 other systems. These include 19 systems external to DHS (e.g., those provided

by commercial entities or other federal government agencies) and 19 systems internal to DHS or FEMA. Some of the internal FEMA systems are undergoing their own modernization efforts and will need to be coordinated with GMM, such as the agency's financial management systems, national flood insurance systems, and enterprise data warehouses.

For example, FEMA's Financial Systems Modernization Program was originally expected to deliver a new financial system in time to interface with GMM. However, the financial modernization has been delayed until after GMM is to be fully implemented; thus, GMM will instead need to interface with the legacy financial system. As a result, GMM is in the process of removing one of its key performance parameters in the acquisition program baseline related to financial systems interoperability and timeliness of data exchanged.

In May 2017, DHS approved the acquisition program baseline for GMM. The baseline estimated the total lifecycle costs to be about $251 million, initial operational capability to be achieved by September 2019, and full operational capability to be achieved by September 2020.

GMM's Agile Software Development and Acquisition Approach

FEMA intends to develop and deploy its own software applications for GMM using a combination of commercial-off-the-shelf software, open source software, and custom developed code.[23] The agency plans to rely on an Agile software development approach. According to FEMA planning documentation, the agency plans to fully deliver GMM by September 2020 over eight Agile development increments.[24]

Agile development is a type of incremental development, which calls for the rapid delivery of software in small, short increments. Many organizations, especially in the federal government, are accustomed to using a waterfall software development model. This type of model

[23]Open source software is publicly available for use, study, reuse, modification, enhancement, and redistribution by the software's users.

[24]Agile development programs may use different terminology to describe their software development processes. The Agile terms used in this report (e.g., increment, sprint, epics, etc.) are specific to the GMM program.

typically consists of long, sequential phases, and differs significantly from the Agile development approach. We have previously reported that DHS has sought to establish Agile software development as the preferred method for acquiring and delivering IT capabilities.[25] However, the department has not yet completed critical actions necessary to update its guidance, policies, and practices for Agile programs, in areas such as, developing lifecycle cost estimates, managing IT requirements, testing and evaluation, oversight at key decision points, and ensuring cybersecurity.[26] (See appendix III for more details on the Agile software development approach.)

FEMA's acquisition approach includes using contract support to assist with the development and deployment efforts. The agency selected a public cloud environment to host the computing infrastructure.[27] In addition, from March through July 2017, the agency used a short-term contract aimed at developing prototypes of GMM functionality for grant tracking and monitoring, case management of disaster survivors, grant reporting, and grant closeout. The agency planned to award a second development contract by December 2017 to complete the GMM system (beyond the prototypes) and to begin this work in September 2018.

However, due to delays in awarding the second contract to develop the complete GMM system, in January 2018, the program extended the scope and time frames of the initial short-term prototype contract for an additional year to develop the first increment of the GMM system—referred to as the AFG pilot.

On August 31, 2018, FEMA awarded the second development contract, which is intended to deliver the remaining functionality beyond the AFG pilot (i.e., increments 2 through 8). FEMA officials subsequently issued a 90-day planning task order for the Agile development contractor to define the work that needs to be done to deliver GMM and the level of effort

[25]GAO, *TSA Modernization: Use of Sound Program Management and Oversight Practices Is Needed to Avoid Repeating Past Problems,* GAO-18-46 (Washington, D.C.: Oct. 17, 2017).

[26]We have an ongoing review evaluating DHS's Agile adoption.

[27]According to NIST, cloud computing is a means for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. A public cloud is a type of deployment model for providing cloud services that is available to the general public and is owned and operated by the service provider.

needed to accomplish that work. However, the planning task order was paused after a bid protest was filed with GAO in September 2018.[28] According to FEMA officials, they resumed work on the planning task order after the bid protest was withdrawn by the protester on November 20, 2018, and then the work was paused again during the partial government shutdown from December 22, 2018, through January 25, 2019.

Assistance to Firefighters Grants Pilot

FEMA began working on the AFG pilot—GMM's first increment—in January 2018. This increment was intended to pilot GMM's use of Agile development methods to replace core functionality for the AFG system (i.e., one of the 10 legacy systems).This system supports three preparedness/fire-related grant programs—Assistance to Firefighters Grants Program, Fire Prevention and Safety Grant Program, and Staffing for Adequate Fire and Emergency Response Grant Program. According to FEMA officials, the AFG system was selected as the first system to be replaced because it is costly to maintain and the DHS OIG had identified cybersecurity concerns with the system.[29]

Among the 43 GMM business functions discussed earlier in this report, FEMA officials specified 19 functions to be delivered in the AFG pilot. Figure 4 shows the planned time frames for delivering the AFG pilot in increment 1 (which consisted of four 3-month Agile development sub-increments), as of August 2018.

[28]GAO's statutory bid protest function is separate from its audit mission.

[29]See for example, DHS OIG, *Security Concerns with Federal Emergency Management Agency's eGrants Grant Management System*, OIG-16-11 (Washington, D.C.: Nov. 19, 2015).

Figure 4: Planned Functionality for the Federal Emergency Management Agency's Assistance to Firefights Grants Pilot, as of August 2018

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

As of August 2018, the program was working on sub-increment 1C of the pilot.[30] In September 2018, GMM deployed its first set of functionality to a total of 19 AFG users—which included seven of 169 total internal AFG

[30]These increments consist of many shorter iterations that are referred to as sprints, during which development teams build a small iteration of working software. As of August 2018, the program had completed 12 sprints. Since Agile programs plan and prioritize requirements iteratively, the total number of sprints to be completed for an entire program is unknown.

users, and 12 of more than 153,000 external AFG users. The functionality supported four of the 19 business functions that are related to the closeout of grants (i.e., the process by which all applicable administrative actions and all required work to award a grant have been completed). This functionality included tasks such as evaluation of final financial reports submitted by grant recipients and final reconciliation of finances (e.g., final disbursement to recipients and return of unobligated federal funds).

According to FEMA officials, closeout functionality was selected first for deployment because it was the most costly component of the legacy AFG system to maintain, as it is an entirely manual and labor-intensive process. The remaining AFG functionality and remaining AFG users are to be deployed by the end of the AFG pilot.

GMM Oversight Structure

The GMM program is executed by a program management office, which is overseen by a program manager and program executive. This office is responsible for directing the day-to-day operations and ensuring completion of GMM program goals and objectives. The program office resides within the Office of Response and Recovery, which is headed by an Associate Administrator who reports to the FEMA Administrator. In addition, the GMM program executive (who is also the Regional Administrator for FEMA Region IX) reports directly to the FEMA Administrator.

GMM is designated as a level 2 major acquisition,[31] which means that it is subject to oversight by the DHS acquisition review board. The board is chaired by the DHS Undersecretary for Management and is made up of executive-level members, such as the DHS Chief Information Officer.

The acquisition review board serves as the departmental executive board that decides whether to approve GMM through key acquisition milestones and reviews the program's progress and its compliance with approved

[31]According to DHS policy, a level 2 investment has a lifecycle cost estimate that is greater than or equal to $300 million and less than $1 billion, or has been designated to be of special interest, which automatically increases the program to at least a level 2 investment. While GMM's initial cost estimate was below the level 2 threshold, it was considered to be of special interest to the DHS Chief Financial Officer because it is a critical element of the department's financial system modernization efforts.

documentation every 6 months. The board approved the acquisition program baseline for GMM in May 2017 (i.e., estimated costs to be about $251 million and full operational capability to be achieved by September 2020).

In addition, the program is reviewed on a monthly basis by FEMA's Grants Management Executive Steering Group. This group is chaired by the Deputy Administrator of FEMA. Further, DHS's Financial Systems Modernization Executive Steering Committee, chaired by the DHS Chief Financial Officer, meets monthly and is to provide guidance, oversight, and support to GMM.

Cybersecurity Risk Management Framework

For government organizations, including FEMA, cybersecurity is a key element in maintaining the public trust. Inadequately protected systems may be vulnerable to insider threats. Such systems are also vulnerable to the risk of intrusion by individuals or groups with malicious intent who could unlawfully access the systems to obtain sensitive information, disrupt operations, or launch attacks against other computer systems and networks. Moreover, cyber-based threats to federal information systems are evolving and growing. Accordingly, we designated cybersecurity as a government-wide high risk area 22 years ago, in 1997, and it has since remained on our high-risk list.[32]

Federal law and guidance specify requirements for protecting federal information and information systems. The Federal Information Security Modernization Act (FISMA) of 2014 requires executive branch agencies to develop, document, and implement an agency-wide cybersecurity program to provide security for the information and information systems that support operations and assets of the agency.[33]

[32]GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: Feb. 1, 1997).

[33]The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

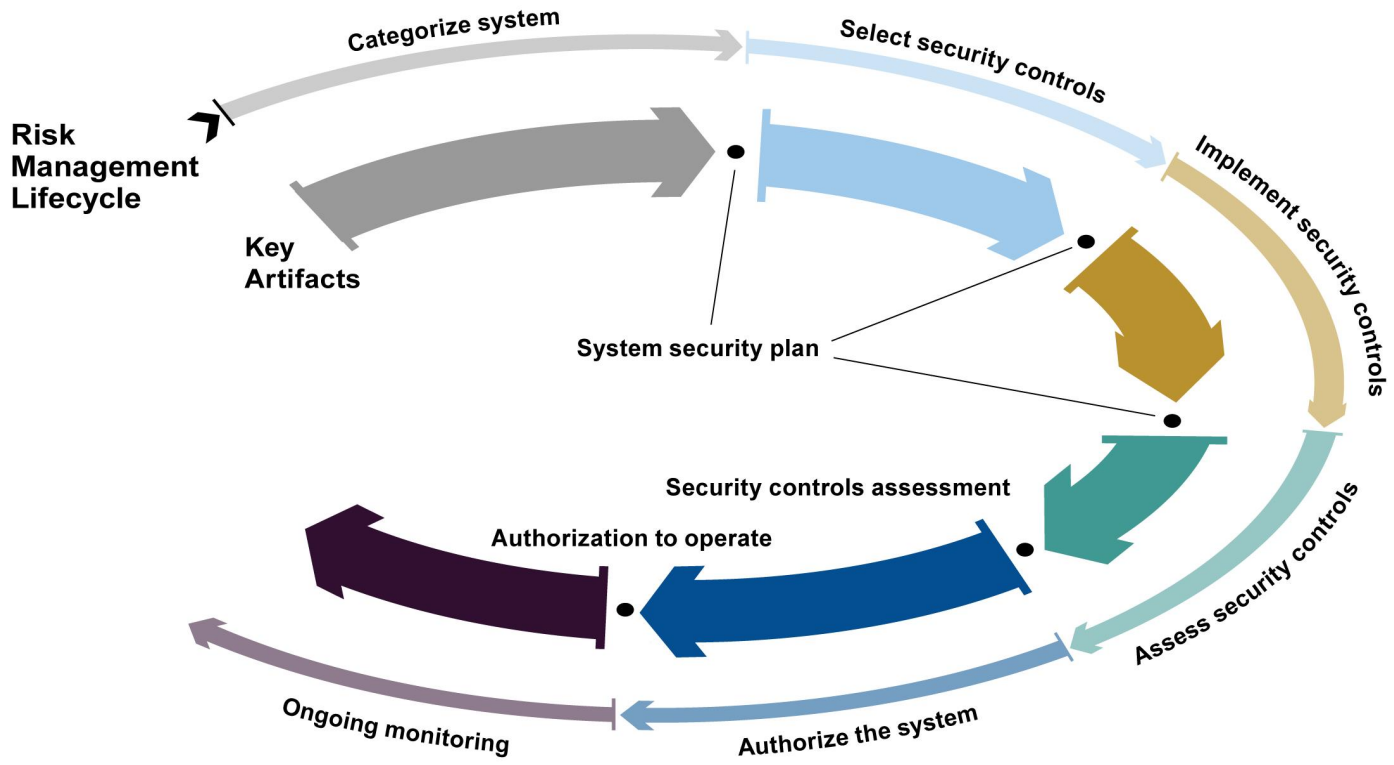
The act also tasks NIST with developing, for systems other than those for national security, standards and guidelines to be used by all agencies to establish minimum cybersecurity requirements for information and information systems based on their level of cybersecurity risk.[34] Accordingly, NIST developed a risk management framework of standards and guidelines for agencies to follow in developing cybersecurity programs.[35]

The framework addresses broad cybersecurity and risk management activities, including categorizing the system's impact level; selecting, implementing, and assessing security controls; authorizing the system to operate (based on progress in remediating control weaknesses and an assessment of residual risk); and monitoring the efficacy of controls on an ongoing basis. Figure 5 provides an overview of this framework.

[34]40 U.S.C. § 11331(b).

[35]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

Figure 5: Overview of the National Institute of Standards and Technology's Risk Management Framework for a Cybersecurity Program



Sources: GAO and National Institute of Standards and Technology. | GAO-19-164

Prior DHS OIG assessments, such as the annual evaluation of DHS's cybersecurity program, have identified issues with FEMA's cybersecurity practices.[36] For example, in 2016, the OIG reported that FEMA was operating 111 systems without an authorization to operate. In addition, the agency had not created any corrective action plans for 11 of the systems that were classified as "Secret" or "Top Secret," thus limiting its ability to ensure that all identified cybersecurity weaknesses were mitigated in a timely manner. The OIG further reported that, for several years, FEMA was consistently below DHS's 90 percent target for remediating corrective action plans, with scores ranging from 73 to 84

[36]See for example, DHS OIG, *Evaluation of DHS's Information Security Program for Fiscal Year 2016*, OIG-17-24 (Washington, D.C.: Jan. 18, 2017); *Evaluation of DHS's Information Security Program for Fiscal Year 2015*, OIG-16-08 (Washington, D.C.: Jan. 5, 2016); and *Evaluation of DHS's Information Security Program for Fiscal Year 2014*, OIG-15-16 (Washington, D.C.: Dec. 12, 2014).

percent. Further, the OIG reported that FEMA had a significant number of open corrective action plans (18,654) and that most of these plans did not contain sufficient information to address identified weaknesses.

In 2017, the OIG reported that FEMA had made progress in addressing security weaknesses. For example, it reported that the agency had reduced the number of systems it was operating without an authorization to operate from 111 to 15 systems.

FEMA Has Implemented Most Leading Practices for Reengineering Grants Management Business Processes and Managing IT Requirements

According to GAO's Business Process Reengineering Assessment Guide and the Software Engineering Institute's Capability Maturity Model Integration® for Development, successful business process reengineering can enable agencies to replace their inefficient and outmoded processes with streamlined processes that can more effectively serve the needs of the public and significantly reduce costs and improve performance.[37] Many times, new IT systems are implemented to support these improved business processes. Thus, effective management of IT requirements is critical for ensuring the successful design, development, and delivery of such new systems.

These leading practices state that effective business process reengineering and IT requirements management involve, among other things, (1) ensuring strong executive leadership support for process reengineering; (2) assessing the current and target business environment and business performance goals; (3) establishing plans for implementing new business processes; (4) establishing clear, prioritized, and traceable IT requirements; (5) tracking progress in delivering IT requirements; and (6) incorporating input from end user stakeholders.

[37]GAO, *Business Process Reengineering Assessment Guide*—Version 3, GAO/AIMD-10.1.15 (Washington, D.C.: May 1997); Software Engineering Institute, *Capability Maturity Model® Integration for Development*, Version 1.3 (Pittsburgh, Pa.: November 2010); and draft *GAO Agile Assessment Guide*, Version 6A.

Among these six selected leading practices for reengineering business processes and managing IT requirements, FEMA fully implemented four and partially implemented two of them for its GMM program. For example, the agency ensured strong senior leadership commitment to changing the way it manages its grants, took steps to assess and document its business environment and performance goals, defined initial IT requirements for GMM, took recent actions to better track progress in delivering planned IT requirements, and incorporated input from end user stakeholders.

In addition, FEMA had begun planning for business process reengineering; however, it had not finalized plans for transitioning users to the new business processes. Further, while GMM took steps to establish clearly defined and prioritized IT requirements, key requirements were not always traceable. Table 3 summarizes the extent to which FEMA implemented the selected leading practices.

Table 3: 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	Fully implemented
Assess the current and target business environment and business performance goals	Fully implemented
Establish plans for implementing new business processes	Partially implemented
Establish clear, prioritized, and traceable IT requirements	Partially implemented
Track progress in delivering IT requirements	Fully implemented
Incorporate input from end user stakeholders	Fully implemented

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

FEMA Executive Leadership Demonstrated Strong Commitment to Reengineering Grants Management Processes

According to GAO's Business Process Reengineering Assessment Guide,[38] the most critical factor for engaging in a reengineering effort is having strong executive leadership support to establish credibility regarding the seriousness of the effort and to maintain the momentum as the agency faces potentially extensive changes to its organizational structure and values. Without such leadership, even the best process design may fail to be accepted and implemented. Agencies should also ensure that there is ongoing executive support (e.g., executive steering committee meetings headed by the agency leader) to oversee the reengineering effort from start to finish.

FEMA senior leadership consistently demonstrated its commitment and support for streamlining the agency's grants management business processes and provided ongoing executive support. For example, one of the Administrator's top priorities highlighted in FEMA's 2014 through 2022 strategic plans was to strengthen grants management through innovative systems and business processes to rapidly and effectively deliver the agency's mission. In accordance with this strategic priority, FEMA initiated GMM with the intent to streamline and modernize grants management across the agency.

In addition, FEMA established the Grants Management Executive Steering Group in September 2015. This group is responsible for transforming the agency's grants management capabilities through its evaluation, prioritization, and oversight of grants management modernization programs, such as GMM.[39] The group's membership consists of FEMA senior leaders from across the agency's program and business support areas, such as FEMA regions, Individual Assistance, Public Assistance, Preparedness, Office of the Chief Financial Officer,

[38]GAO/AIMD-10.1.15.

[39]According to DHS officials, the Grants Management Executive Steering Group is also intended to address a recommendation from the DHS OIG that FEMA assign the responsibility for central oversight of grants management to one program office to ensure that there is effective management and administration of the grants process, as well as ensuring effective implementation of the provisions of 31 U.S.C. §§ 7501-06 (see for example, DHS OIG-18-16).

Office of Chief Counsel, OCIO, and the Office of Policy and Program Analysis. In this group's ongoing commitment to reengineering grants management processes, it meets monthly to review GMM's updates, risks, and action items, as well as the program's budget, schedule, and acquisition activities. For example, the group reviewed the status of key acquisition activities and program milestones, such as the follow-on award for the pilot contractor and the program's initial operational capability date. The group also reviewed GMM's program risks, such as data migration challenges (discussed later in this report) and delays in the Agile development contract award. With this continuous executive involvement, FEMA is better positioned to maintain momentum for reengineering the new grants management business processes that the GMM system is intended to support.

FEMA Documented Its Current and Target Grants Management Business Processes and Performance Improvement Goals

GAO's Business Process Reengineering Assessment Guide[40] states that agencies undergoing business process reengineering should develop a common understanding of the current environment by documenting existing core business processes to show how the processes work and how they are interconnected. The agencies should then develop a deeper understanding of the target environment by modeling the workflow of each target business process in enough detail to provide a common understanding of exactly what will be changed and who will be affected by a future solution. Agencies should also assess the performance of their current major business processes to identify problem areas that need to be changed or eliminated and to set realistically achievable, customer-oriented, and measurable business performance improvement goals.

FEMA has taken steps to document the current and target grants management business processes. Specifically,

- The agency took steps to develop a common understanding of its grants management processes by documenting each of the 12 grant categories. For example, in 2016 and 2017, the agency conducted several nationwide user outreach sessions with representatives from FEMA headquarters, the 10 regional offices, and state and local grant

[40]GAO/AIMD-10.1.15.

recipients to discuss the grant categories and the current grants management business environment.

In addition, FEMA's Office of Chief Counsel developed a Grants Management Manual in January 2018 that outlined the authorizing laws, regulations, and agency policies for all of its grant programs. According to the Grants Management Executive Steering Group, the manual is intended to promote standardized grants management procedures across the agency. Additionally, the group expects grant program and regional offices to assess the manual against their own practices, make updates as needed, and ensure that their staff are properly informed and trained.

- FEMA also documented target grants management business process workflows for 18 of the 19 business functions that were notionally planned to be developed and deployed in the AFG pilot by December 2018.[41] However, the program experienced delays in developing the AFG pilot (discussed later in this report) and, thus, deferred defining the remaining business function until the program gets closer to developing that function, which is now planned for August 2019.

In addition, FEMA established measurable business performance goals for GMM that are aimed at addressing problem areas and improving grants management processes. Specifically, the agency established 14 business performance goals and associated thresholds in an October 2017 acquisition program baseline addendum, as well as 126 performance metrics for all 43 of the target grants management business functions in its March 2017 test and evaluation master plan.

According to FEMA, the 14 business performance goals are intended to represent essential outcomes that will indicate whether GMM has successfully met critical, business-focused mission needs. GMM performance goals include areas such as improvements in the satisfaction level of users with GMM compared to the legacy systems and improvements in the timeliness of grant award processing. For example, one of GMM's goals is to get at least 40 percent of users surveyed to agree or strongly agree that their grants management business

[41]While the pilot was originally intended to deliver just the IT infrastructure for GMM, the program later decided that it would also attempt to replace core functionality for AFG. This core functionality consisted of 19 of 33 total GMM business functions that are needed for the AFG program. The remaining 14 business functions are to be delivered to the AFG program sometime after the pilot, based on priorities set by GMM stakeholders.

processes are easier to accomplish with GMM, compared to the legacy systems.

Program officials stated that they plan to work with the Agile development contractor to refine their performance goals and target thresholds, develop a plan for collecting the data and calculating the metrics, and establish a performance baseline with the legacy systems. Program officials also stated that they plan to complete these steps by September 2019—GMM's initial operational capability date—which is when they are required to begin reporting these metrics to the DHS acquisition review board.

FEMA Has Begun Planning Its Grants Management Business Process Reengineering, but Has Not Finalized Plans for Transition Activities

According to GAO's Business Process Reengineering Assessment Guide,[42] agencies undergoing business process reengineering should (1) establish an overall plan to guide the effort (commonly referred to as an organizational change management plan) and (2) provide a common understanding for stakeholders of what to expect and how to plan for process changes. Agencies should develop the plan at the beginning of the reengineering effort and provide specific details on upcoming process changes, such as critical milestones and deliverables for an orderly transition, roles and responsibilities for change management activities, reengineering goals, skills and resource needs, key barriers to change, communication expectations, training, and any staff redeployments or reductions-in-force. The agency should develop and begin implementing its change management plan ahead of introducing new processes to ensure sufficient support among stakeholders for the reengineered processes.

While FEMA has begun planning its business process reengineering activities, it has not finalized its plans or established time frames for their completion. Specifically, as of September 2018, program officials were in the process of drafting an organizational change management plan that is intended to establish an approach for preparing grants management stakeholders for upcoming changes. According to FEMA, this document is intended to help avoid uncertainty and confusion among stakeholders

[42]GAO/AIMD-10.1.15.

as changes are made to the agency's grant programs, and ensure successful adoption of new business processes, strategies, and technologies.

As discussed previously in this report, the transition to GMM will involve changes to FEMA's disparate grants management processes that are managed by many different stakeholders across the agency. Program officials acknowledged that change management is the biggest challenge they face in implementing GMM and said they had begun taking several actions intended to support the agency's change management activities. For example, program officials reported in October 2018 that they had recently created an executive-level working group intended to address FEMA's policy challenges related to the standardization of grants management processes. Additionally, program officials reported that they planned to: (1) hire additional support staff focused on coordinating grants change management activities; and (2) pursue regional office outreach to encourage broad support among GMM's decentralized stakeholders, such as state, local, and tribal territories.

However, despite these actions, the officials were unable to provide time frames for completing the organizational change management plan or the additional actions. Until the plan and actions are complete, the program lacks assurance that it will have sufficient support among stakeholders for the reengineered processes.

In addition, GMM did not establish plans and time frames for the activities that needed to take place prior to, during, and after the transition from the legacy AFG to GMM. Instead, program officials stated that they had worked collaboratively with the legacy AFG program and planned these details informally by discussing them in various communications, such as emails and meetings. However, this informal planning approach is not a repeatable process, which is essential to this program as FEMA plans to transition many sets of functionality to many different users during the lifecycle of this program.

Program officials acknowledged that for future transitions they will need more repeatable transition planning and stated that they intend to establish such plans, but did not provide a time frame for when such changes would be made. Until FEMA develops a repeatable process, with established time frames for communicating the transition details to its customers prior to each transition, the agency risks that the transition from the legacy systems to GMM will not occur as intended. It also

increases its risk that stakeholders will not support the implementation of reengineered grants management processes.

GMM Took Steps to Establish Clearly Defined and Prioritized IT Requirements, but Key Requirements Were Not Always Traceable

Leading practices for software development efforts state that IT requirements are to be clearly defined and prioritized.[43] This includes, among other things, maintaining bidirectional traceability as the requirements evolve, to ensure there are no inconsistencies among program plans and requirements.[44] In addition, programs using Agile software development are to maintain a product vision, or roadmap, to guide the planning of major program milestones and provide a high-level view of planned requirements.[45]

Programs should also maintain a prioritized list (referred to as a backlog) of narrowly defined requirements (referred to as lower-level requirements) that are to be delivered. Programs should maintain this backlog with the product owner to ensure the program is always working on the highest priority requirements that will deliver the most value to the users.[46]

The GMM program established clearly defined and prioritized requirements and maintained bidirectional traceability among the various levels of requirements:

- Grant lifecycle phases: In its Concept of Operations document, the program established six grants management lifecycle phases that

[43]Software Engineering Institute, *Capability Maturity Model® Integration for Development*, Version 1.3 (Pittsburgh, Pa.: November 2010); and draft *GAO Agile Assessment Guide*, Version 6A.

[44]Bidirectional traceability refers to a discernable association in either direction between different levels of IT requirements, as well as between IT requirements and related work products.

[45]Agile programs may have multiple artifacts depicting the program's milestones and planned requirements. For reporting purposes, we referred to these collectively as GMM's "roadmap."

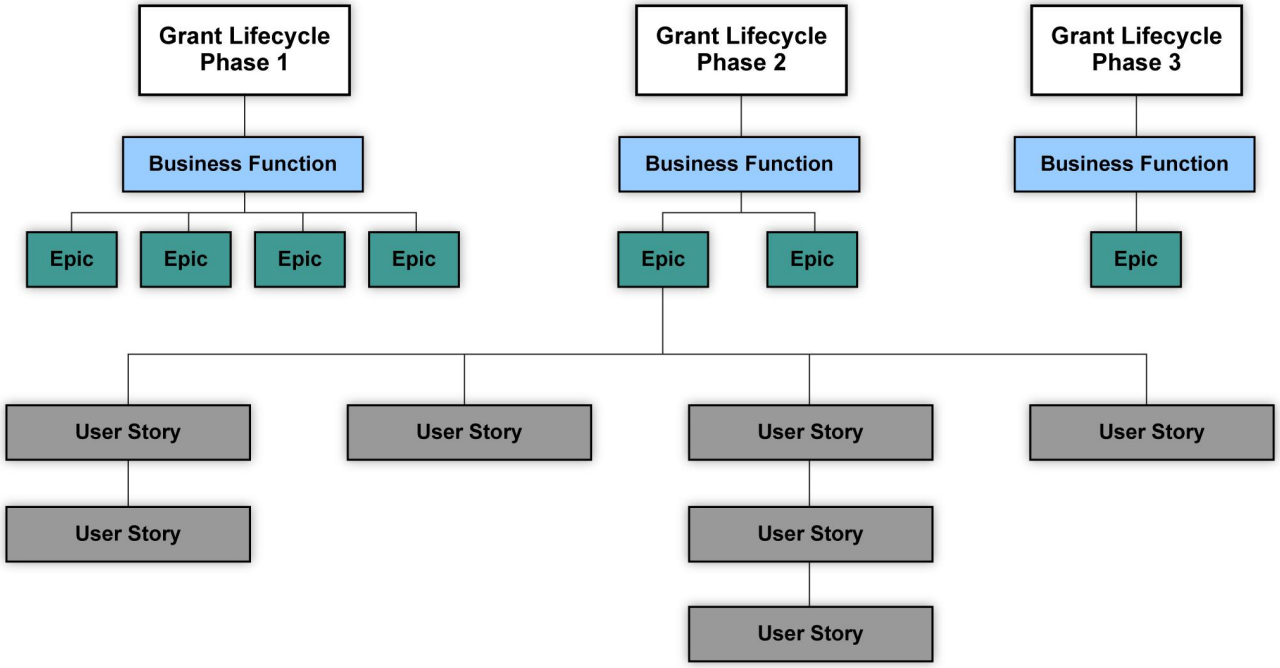
[46]Product owners represent the end users of the system and they work closely with the Agile development teams to establish priorities based on business needs, clarify the IT requirements, and approve whether completed work meets those requirements.

represent the highest level of GMM's requirements, through which it derives lower-level requirements.

- Business functions: The Concept of Operations document also identifies the next level of GMM requirements—the 43 business functions that describe how FEMA officials, grant recipients, and other stakeholders are to manage grants. According to program officials, the 43 business functions are to be refined, prioritized, and delivered to GMM customers iteratively. Further, for the AFG pilot, the GMM program office prioritized 19 business functions with the product owner and planned the development of these functions in a roadmap.
- Epics: GMM's business functions are decomposed into epics, which represent smaller portions of functionality that can be developed over multiple increments. According to program officials, GMM intends to develop, refine, and prioritize the epics iteratively. As of August 2018, the program had developed 67 epics in the program backlog. An example of one of the epics for the AFG pilot is to prepare and submit grant closeout materials.
- User stories: The epics are decomposed into user stories, which convey the customers' requirements at the smallest and most discrete unit of work that must be done within a single sprint to create working software. GMM develops, refines, and prioritizes the user stories iteratively. As of August 2018, the program had developed 1,118 user stories in the backlog. An example of a user story is "As an external user, I can log in with a username and password."

Figure 6 provides an example of how GMM's different levels of requirements are decomposed.

Figure 6: Example of the Decomposition of Information Technology Requirements for the Federal Emergency Management Agency's Grants Management Modernization Program



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

Nevertheless, while we found requirements to be traceable at the sprint-level (i.e., epics and user stories), traceability of requirements at the increment-level (i.e., business functions) were inconsistent among different requirements planning documents.[47] Specifically, the capabilities and constraints document shows that five business functions are planned to be developed within sub-increment 1A, whereas the other key planning document—the roadmap for the AFG pilot—showed one of those five functions as being planned for the sub-increment 1B. In addition, the capabilities and constraints document shows that nine business functions are planned to be developed within sub-increment 1B, but the roadmap showed one of those nine functions as being planned for the sub-increment 1C.

[47]GMM's sprints are shorter periods of time (weeks) and increments are longer periods of time (months), in which the requirements that will be developed within that time period are planned in advance.

Program officials stated that they decided to defer these functions to later sub-increments due to unexpected technical difficulties encountered when developing functionality and reprioritizing functions with the product owners.[48] While the officials updated the roadmap to reflect the deferred functionality, they did not update the capabilities and constraints document to maintain traceability between these two important requirements planning documents.

Program officials stated that they learned during the AFG pilot that the use of a capabilities and constraints document for increment-level scope planning was not ideal and that they intended to change the process for how they documented planned requirements for future increments. However, program officials did not provide a time frame for when this change would be made. Until the program makes this change and then ensures it maintains traceability of increment-level requirements between requirements planning documents, it will continue to risk confusion among stakeholders about what is to be delivered.

In addition, until recently, GMM's planning documents were missing up-to-date information regarding when most of the legacy systems will be transitioned to GMM. Specifically, while the program's planning documents (including the GMM roadmap) provided key milestones for the entire lifecycle of the program and high-level capabilities to be delivered in the AFG pilot, these documents lacked up-to-date time frames for when FEMA planned to transition the nine remaining legacy systems. For example, in May 2017, GMM drafted notional time frames for transitioning the legacy systems, including plans for AFG to be the seventh system replaced by GMM. However, in December 2017, the program decided to reprioritize the legacy systems so that AFG would be replaced first—yet this major change was not reflected in the program's roadmap.

Moreover, while AFG program officials were informed of the decision to transition the AFG program first, in June 2018 officials from other grant programs told us that they had not been informed on when their systems were to be replaced. As a result, these programs were uncertain about when they should start planning for their respective transitions. In August 2018, GMM program officials acknowledged that they were delayed in deciding the sequencing order for the legacy system transitions. Program

[48]Increment 1 was originally intended to deliver just the IT infrastructure for GMM. The program later decided that it would also attempt to replace core functionality for the AFG system—which was the functionality that was deferred.

officials stated that the delay was due to their need to factor the Agile development contractor's perspective into these decisions; yet, at that time, the contract award had been delayed by approximately 8 months. Subsequently, in October 2018, program officials identified tentative time frames for transitioning the remaining legacy systems.

Program officials stated that they determined the tentative time frames for transitioning the legacy systems based on key factors, such as mission need, cost, security vulnerabilities, and technical obsolescence, and that they had shared these new time frames with grant program officials. The officials also stated that, once the Agile contractor begins contract performance, they expect to be able to validate the contractor's capacity and finalize these time frames by obtaining approval from the Grants Management Executive Steering Group. By taking steps to update and communicate these important time frames, FEMA should be better positioned to ensure that each of the grant programs are prepared for transitioning to GMM.

GMM Recently Began Tracking Progress in Delivering Planned IT Requirements

According to leading practices,[49] Agile programs should track their progress in delivering planned IT requirements within a sprint (i.e., short iterations that produce working software). Given that sprints are very short cycles of development (e.g., 2 weeks), the efficiency of completing planned work within a sprint relies on a disciplined approach that includes using a fixed pace, referred to as the sprint cadence, that provides a consistent and predictable development routine. A disciplined approach also includes identifying by the start of a sprint which user stories will be developed, developing those stories to completion (e.g., fully tested and demonstrated to, and accepted by, the product owner), and tracking completion progress of those stories. Progress should be communicated to relevant stakeholders and used by the development teams to better understand their capacity to develop stories, continuously improve on their processes, and forecast how long it will take to deliver all remaining capabilities.

[49]Software Engineering Institute, *Capability Maturity Model® Integration for Development*, Version 1.3 (Pittsburgh, Pa.: November 2010); and draft *GAO Agile Assessment Guide*, Version 6A.

The GMM program did not effectively track progress in delivering IT requirements during the first nine sprints, which occurred from January to June 2018. These gaps in tracking the progress of requirements, in part, had an impact on the program's progress in delivering the 19 AFG business functions that were originally planned by December 2018 and are now deferred to August 2019. However, beginning in July 2018, in response to our ongoing review, the program took steps to improve in these areas. Specifically,

- GMM did not communicate the status of its Agile development progress to program stakeholders, such as the grant programs, the regional offices, and the development teams, during most of the first nine sprints. Program officials acknowledged that they should use metrics to track development progress and, in July 2018, they began reporting metrics to program stakeholders. For example, they began collecting and providing data on the number of stories planned and delivered, estimated capacity for development teams, and the number of days spent working on the sprint, as part of the program's weekly status reports to program stakeholders, such as product owners.
- Rather than using a fixed, predictable sprint cadence, GMM allowed a variable development cadence, meaning that sprint durations varied from 1 to 4 weeks throughout the first nine sprints. Program officials noted that they had experimented with the use of a variable cadence to allow more time to complete complex technical work. Program officials stated that they realized that varying the sprints was not effective and, in July 2018 for sprint 10, they reverted back to a fixed, 2 week cadence.
- GMM added a significant amount of scope during its first nine sprints, after the development work had already begun. For example, the program committed to 28 user stories at the beginning of sprint eight, and then nearly doubled the work by adding 25 additional stories in the middle of the sprint. Program officials cited multiple reasons for adding more stories, including that an insufficient number of stories had been defined in the backlog when the sprint began, the realization that planned stories were too large and needed to be decomposed into smaller stories, and the realization that other work would be needed in addition to what was originally planned. Program officials recognized that, by the start of a sprint, the requirements should be sufficiently defined, such that they are ready for development without requiring major changes during the sprint. The program made recent improvements in sprints 11 and 12, which had only five stories added after the start of a sprint.

By taking these steps to establish consistency among sprints, the program has better positioned itself to more effectively monitor and manage the remaining IT development work. In addition, this improvement in consistency should help the program avoid future deferments of functionality.

GMM Is Involving Stakeholders and Incorporating Input

Leading practices state that programs should regularly collaborate with, and collect input from, relevant stakeholders; monitor the status of stakeholder involvement; incorporate stakeholder input; and measure how well stakeholders' needs are being met.[50] For Agile programs, it is especially important to track user satisfaction to determine how well the program has met stakeholders' needs. Consistent stakeholder participation ensures that the program meets its stakeholders' needs.

FEMA implemented its responsibilities in this area through several means, such as stakeholder outreach activities; development of a strategic communications plan; and continuous monitoring, solicitation, and recording of stakeholder involvement and feedback. For example, the agency conducted nationwide outreach sessions from January 2016 through August 2017 and began conducting additional outreach sessions in April 2018. These outreach sessions involved hundreds of representatives from FEMA headquarters, the 10 regional offices, and state and local grant recipients to collect information on the current grants management environment and opportunities for streamlining grants management processes.

FEMA also held oversight and stakeholder outreach activities and actively solicited and recorded feedback from its stakeholders on a regular basis. For example, GMM regularly verified with users that the new functionality met their IT requirements, as part of the Agile development cycle. Additionally, we observed several GMM biweekly requirements validation sessions where the program's stakeholders were involved and provided feedback as part of the requirements development and refinement process.

[50]Software Engineering Institute, *Capability Maturity Model® Integration for Development*, Version 1.3 (Pittsburgh, Pa.: November 2010); and draft *GAO Agile Assessment Guide*, Version 6A.

In addition, FEMA identified GMM stakeholders and tracked its engagement with these stakeholders using a stakeholder register. The agency also defined processes for how the GMM program is to collaborate with its stakeholders in a stakeholder communication plan and Agile development team agreement. Also, while several officials from the selected grant program and regional offices that we interviewed indicated that the program could improve in communicating its plans for GMM and incorporating stakeholder input, most of the representatives from these offices stated that GMM is doing well at interacting with its stakeholders.

Finally, in October 2018, program officials reported that they had recently begun measuring user satisfaction by conducting surveys and interviews with users that have utilized the new functionality within GMM. The program's outreach activities, collection of stakeholder input, and measurement of user satisfaction demonstrate that the program is taking the appropriate steps to incorporate stakeholder input.

FEMA Lacks a Current Cost Estimate and Reliable Schedule for GMM

GMM's Initial Cost Estimate Was Reliable, but Is Now Outdated

Reliable cost estimates are critical for successfully delivering IT programs. Such estimates provide the basis for informed decision making, realistic budget formulation, meaningful progress measurement, and accountability for results. GAO's Cost Estimating and Assessment Guide defines leading practices related to the following four characteristics of a high-quality, reliable estimate.[51]

- Comprehensive. The estimate accounts for all possible costs associated with a program, is structured in sufficient detail to ensure that costs are neither omitted nor double counted, and documents all cost-influencing assumptions.
- Well-documented. Supporting documentation explains the process, sources, and methods used to create the estimate; contains the

[51]GAO-09-3SP.

underlying data used to develop the estimate; and is adequately reviewed and approved by management.

- Accurate. The estimate is not overly conservative or optimistic, is based on an assessment of the costs most likely to be incurred, and is regularly updated so that it always reflects the program's current status.
- Credible. Discusses any limitations of the analysis because of uncertainty or sensitivity surrounding data or assumptions, the estimate's results are cross-checked, and an independent cost estimate is conducted by a group outside the acquiring organization to determine whether other estimating methods produce similar results.

In May 2017, DHS approved GMM's lifecycle cost estimate of about $251 million for fiscal years 2015 through 2030. We found this initial estimate to be reliable because it fully or substantially addressed all the characteristics associated with a reliable cost estimate. For example, the estimate comprehensively included government and contractor costs, all elements of the program's work breakdown structure, and all phases of the system lifecycle; and was aligned with the program's technical documentation at the time the estimate was developed. GMM also fully documented the key assumptions, data sources, estimating methodology, and calculations for the estimate. Further, the program conducted a risk assessment and sensitivity analysis, and DHS conducted an independent assessment of the cost estimate to validate the accuracy and credibility of the cost estimate.

However, key assumptions that FEMA made about the program changed soon after DHS approved the cost estimate in May 2017. Thus, the initial cost estimate no longer reflects the current approach for the program. For example, key assumptions about the program that changed include:

- Change in the technical approach: The initial cost estimate assumed that GMM would implement a software-as-a-service model, meaning that FEMA would rely on a service provider to deliver software applications and the underlying infrastructure to run them. However, in December 2017, the program instead decided to implement an infrastructure-as-a-service model, meaning that FEMA would develop and deploy its own software application and rely on a service provider to deliver and manage the computing infrastructure (e.g., servers, software, storage, and network equipment). According to program officials, this decision was made after learning from the Agile prototypes that the infrastructure-as-a-service model would allow GMM to develop the system in a more flexible environment.

- Increase in the number of system development personnel: A key factor with Agile development is the number of development teams (each consisting of experts in software development, testing, and cybersecurity) that are operating concurrently and producing separate portions of software functionality. Program officials initially assumed that they would need three to four concurrent Agile development teams, but subsequently realized that they would instead need to expend more resources to achieve GMM's original completion date. Specifically, program officials now expect they will need to at least double, and potentially triple, the number of concurrent development teams to meet GMM's original target dates.
- Significant delays and complexities with data migration: In 2016 and 2017, GMM experienced various technical challenges in its effort to transfer legacy system data to a data staging platform. This data transfer effort needed to be done to standardize the data before eventually migrating the data to GMM. These challenges resulted in significant delays and cost increases. Program officials reported that, by February 2018—at least 9 months later than planned—all legacy data had been transferred to a data staging platform so that FEMA officials could begin analyzing and standardizing the data prior to migrating it into GMM.

FEMA officials reported that they anticipated the cost estimate to increase, and for this increase to be high enough to breach the $251 million threshold set in GMM's May 2017 acquisition program baseline. Thus, consistent with DHS's acquisition guidance, the program informed the DHS acquisition review board of this anticipated breach. The board declared that the program was in a cost breach status, as of September 12, 2018.

As of October 2018, program officials stated that they were in the process of revising the cost estimate to reflect the changes in the program and to incorporate actual costs. In addition, the officials stated that the program was applying a new cost estimating methodology tailored for Agile programs that DHS's Cost Analysis Division had been developing. In December 2018, program officials stated that they had completed the revised cost estimate but it was still undergoing departmental approval. Establishing an updated cost estimate should help FEMA better understand the expected costs to deliver GMM under the program's current approach and time frames.

GMM's Schedule Is Unreliable

The success of an IT program depends, in part, on having an integrated and reliable master schedule that defines when the program's set of work activities and milestone events are to occur, how long they will take, and how they are related to one another. Among other things, a reliable schedule provides a roadmap for systematic execution of an IT program and the means by which to gauge progress, identify and address potential problems, and promote accountability.

GAO's Schedule Assessment Guide defines leading practices related to the following four characteristics that are vital to having a reliable integrated master schedule.[52]

- Comprehensive. A comprehensive schedule reflects all activities for both the government and its contractors that are necessary to accomplish a program's objectives, as defined in the program's work breakdown structure. The schedule also includes the labor, materials, and overhead needed to do the work and depicts when those resources are needed and when they will be available. It realistically reflects how long each activity will take and allows for discrete progress measurement.
- Well-constructed. A schedule is well-constructed if all of its activities are logically sequenced with the most straightforward logic possible. Unusual or complicated logic techniques are used judiciously and justified in the schedule documentation. The schedule's critical path represents a true model of the activities that drive the program's earliest completion date and total float[53] accurately depicts schedule flexibility.
- Credible. A schedule that is credible is horizontally traceable—that is, it reflects the order of events necessary to achieve aggregated products or outcomes. It is also vertically traceable—that is, activities in varying levels of the schedule map to one another and key dates presented to management in periodic briefings are consistent with the schedule. Data about risks are used to predict a level of confidence in meeting the program's completion date. The level of necessary

[52]GAO-16-89G.

[53]Total float, or slack, in the schedule is based on the amount of time that activities can be delayed before the delay affects the program's estimated completion date.

schedule contingency and high-priority risks are identified by conducting a robust schedule risk analysis.

- Controlled. A schedule is controlled if it is updated regularly by trained schedulers using actual progress and logic to realistically forecast dates for program activities. It is compared to a designated baseline schedule to measure, monitor, and report the program's progress. The baseline schedule is accompanied by a baseline document that explains the overall approach to the program, defines ground rules and assumptions, and describes the unique features of the schedule. The baseline schedule and current schedule are subject to a configuration management control process.

GMM's schedule was unreliable because it minimally addressed three characteristics—comprehensive, credible, and controlled—and did not address the fourth characteristic of a reliable estimate—well-constructed. One of the most significant issues was that the program's fast approaching, 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. Table 4 summarizes our assessment of GMM's schedule.

Table 4: Extent to Which the Federal Emergency Management Agency's (FEMA) Grants Management Modernization (GMM) Program's Schedule Addressed the Characteristics of a Reliable Schedule, as of May 2018

Characteristic	Rating	Summary of assessment
Comprehensive • Captures all activities, as identified in the work breakdown structure, which defines in detail the work for both the government and its contractors necessary to accomplish a program's objectives. • Reflects what resources (e.g., labor, materials, and overhead) are needed to do the work, whether all required resources will be available when needed, and whether any funding or time constraints exist. • Establishes the duration of all activities and has specific start and end dates.	Minimally addressed	The GMM schedule included both government and contractor activities and was aligned at a high level with key milestones established in the acquisition program baseline. However, the schedule's activities did not align with the program's work breakdown structure. Additionally, the schedule contained limited information on the resources needed to complete activities. Program officials stated that they did not include information on resources in the schedule because they did not rely on the schedule to manage its resources. Instead, the officials stated that they planned the work and resources outside of the schedule, as they approached each Agile development cycle sprint. However, sprint-related activities only accounted for about a quarter of the schedule (174 out of 662 days, or approximately 26 percent). Further, the schedule had activities that were missing durations and work that was planned to start or finish on weekends. Finally, the program's final delivery date of September 2020 was not informed by a realistic assessment of GMM development activities. Instead, FEMA's Executive Steering Group decided that GMM would be a 5-year program when it was initiated in 2015. However, schedules that are determined by imposed target completion dates, rather than the work that has to be performed and the dependencies among them, are often infeasible.

Characteristic	Rating	Summary of assessment
Well-constructed • Sequences all activities—that is, all activities are sequenced in the order that they are to be implemented with the most straightforward logic possible. • Establishes a valid critical path, which represents the chain of dependent activities with the longest total duration. A valid critical path is necessary to examine the effects of any activity slippage along this path. • Identifies the total float time—the amount of time by which an activity can slip before the delay affects the program's estimated finish date—so that a schedule's flexibility can be determined.	Not addressed	Approximately 82 percent of the activities were not sequenced in the order that they were to be implemented because they were missing dependencies, meaning that they did not identify other activities in the schedule that must occur before or after that activity. As a result, if the program experienced a delay in an activity, the effect of that change on downstream activities could not be automatically reflected in the schedule. Additionally, about 38 percent of remaining activities had unjustified constraints, meaning that the program manually imposed restrictions on when the activity was allowed to start or finish. According to GAO's Schedule Assessment Guide, such constraints should be used only when necessary and only if their justification is documented because they override schedule logic and restrict how planned dates respond to accomplished effort or resource availability. The lack of scheduling logic prevented the schedule from calculating a valid critical path and created unreasonable total float values. Without a valid critical path, management cannot focus on activities that could detrimentally affect the key program milestones if they slip.
Credible • Verifies that the schedule is (1) horizontally traceable, meaning that it reflects the order of events necessary to achieve aggregated products or outcomes; and (2) vertically traceable, meaning that activities in varying levels of the schedule align with one another and key dates presented to management in periodic briefings are consistent with the schedule. • Conducts a schedule risk analysis to predict a level of confidence in meeting the program's completion date and the level of necessary schedule contingency.	Minimally addressed	While the schedule's high-level dates were consistent with the dates found in other program documents, such as GMM's roadmap and acquisition program baseline, the program had manually imposed restrictions, or constraints, on these activities so that they would start or end at a specific time. However, GAO's Schedule Assessment Guide states that the high-level start and end dates should be automatically derived by the scheduling logic established by lower-level activities in the schedule. Additionally, the schedule was not horizontally or vertically traceable because of the lack of scheduling logic discussed previously in this table. Finally, a formal schedule risk analysis was not completed. Program officials said they were assessing the risks facing the program and mitigating those risks in real time as part of their Agile development process. However, a formal schedule risk analysis focuses on how uncertainty and key risks affect activities in the schedule and uses statistical techniques to predict a level of confidence in meeting the program's completion date. Without such an analysis, FEMA is unable to determine the likelihood of GMM achieving its estimated completion date for the estimated scope, or the paths or activities that are most likely to delay the program.
Controlled • Updates schedule regularly using actual progress and logic to realistically forecast dates for program activities. • Maintains a baseline schedule to measure, monitor, and report the program's progress.	Minimally addressed	While GMM program officials cited ways that the status of activities were tracked and updated weekly and daily, such as by examining impediments that slow down Agile development progress, the schedule itself was not being updated as part of these activities. Additionally, the schedule had numerous date anomalies, including activities with planned dates in the past or actual dates in the future. According to GAO's Schedule Assessment Guide, a schedule that has not been appropriately updated will not reflect what is actually occurring on the program and will prevent management from using the schedule to monitor progress. Further, while program officials stated that they considered the milestones in the acquisition program baseline to serve as their schedule baseline, they did not establish a baseline schedule to measure, monitor, and report progress in the schedule management software. Without continual monitoring of program performance against the baseline, GMM has limited ability to determine when forecasted completion dates differ from baseline dates and whether schedule variances affect downstream work.

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

In discussing the reasons for the shortfalls in these practices, program officials stated that they had been uncertain about the level of rigor that should be applied to the GMM schedule, given their use of Agile development. However, leading practices state that program schedules should meet all the scheduling practices, regardless of whether a program is using Agile development.[54] As discussed earlier in this report, GMM has already experienced significant schedule delays. For example, the legacy data migration effort, the AFG pilot, and the Agile development contract have been delayed.

Program officials also stated that the delay in awarding and starting the Agile contract has delayed other important activities, such as establishing time frames for transitioning legacy systems. A more robust schedule could have helped FEMA predict the impact of delays on remaining activities and identify which activities appeared most critical so that the program could ensure that any risks in delaying those activities were properly mitigated.

In response to our review and findings, program officials recognized the need to continually enhance their schedule practices to improve the management and communication of program activities. As a result, in August 2018, the officials stated that they planned to add a master scheduler to the team to improve the program's schedule practices and ensure that all of the areas of concern we identified are adequately addressed. In October 2018, the officials reported that they had recently added two master schedulers to GMM. According to the statement of objectives, the Agile contractor is expected to develop an integrated master schedule soon after it begins performance.

However, program officials stated that GMM is schedule-driven—due to the Executive Steering Group's expectation that the solution will be delivered by September 2020. The officials added that, if GMM encounters challenges in meeting this time frame, the program plans to seek additional resources to allow it to meet the 2020 target.

GMM's schedule-driven approach has already led to an increase in estimated costs and resources. For example, as previously mentioned, the program has determined that, to meet its original target dates, GMM needs to at least double, and possibly triple, the number of concurrent

[54]GAO-16-89G and draft *GAO Agile Assessment Guide*, Version 6A.

Agile development teams. In addition, we have previously reported that schedule pressure on federal IT programs can lead to omissions and skipping of key activities, especially system testing.[55]

In August 2018, program officials acknowledged that September 2020 may not be feasible and that the overall completion time frames established in the acquisition program baseline may eventually need to be rebaselined. Without a robust schedule to forecast whether FEMA's aggressive delivery goal for GMM is realistic to achieve, leadership will be limited in its ability to make informed decisions on what additional increases in cost or reductions in scope might be needed to fully deliver the system.

FEMA Fully Addressed Three Key Cybersecurity Practices and Partially Addressed Two Others

NIST's risk management framework establishes standards and guidelines for agencies to follow in developing cybersecurity programs.[56] Agencies are expected to use this framework to achieve more secure information and information systems through the implementation of appropriate risk mitigation strategies and by performing activities that ensure that necessary security controls are integrated into agencies' processes. The framework addresses broad cybersecurity and risk management activities, which include the following:

- Categorize the system: Programs are to categorize systems by identifying the types of information used, selecting a potential impact level (e.g., low, moderate, or high), and assigning a category based on the highest level of impact to the system's confidentiality, integrity, and availability, if the system was compromised. Programs are also to document a description of the information system and its boundaries

[55]GAO, *2020 Census: Continued Management Attention Needed to Address Challenges and Risks with Developing, Testing, and Securing IT Systems*, GAO-18-655 (Washington, D.C.: Aug. 30, 2018); and *Information Technology: Census Bureau Testing of 2010 Decennial Systems Can Be Strengthened*, GAO-09-262 (Washington, D.C.: Mar. 5, 2009).

[56]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

and should register the system with appropriate program management offices. System categorization is documented in a system security plan.

- Select and implement security controls: Programs are to determine protective measures, or security controls, to be implemented based on the system categorization results. These security controls are documented in a system security plan. For example, control areas include access controls, incident response, security assessment and authorization, identification and authentication, and configuration management. Once controls are identified, programs are to determine planned implementation actions for each of the designated controls. These implementation actions are also specified in the system security plan.
- Assess security controls: Programs are to develop, review, and approve a security assessment plan. The purpose of the security assessment plan approval is to establish the appropriate expectations for the security control assessment. Programs are to also perform a security control assessment by evaluating the security controls in accordance with the procedures defined in the security assessment plan, in order to determine the extent to which the controls were implemented correctly. The output of this process is intended to produce a security assessment report to document the issues, findings, and recommendations. Programs are to conduct initial remediation actions on security controls and reassess those security controls, as appropriate.[57]
- Obtain an authorization to operate the system: Programs are to obtain security authorization approval in order to operate a system. Resolving weaknesses and vulnerabilities identified during testing is an important step leading up to achieving an authorization to operate. Programs are to establish corrective action plans to address any deficiencies in cybersecurity policies, procedures, and practices. DHS guidance also states that corrective action plans must be developed for every weakness identified during a security control assessment and within a security assessment report.
- Monitor security controls on an ongoing basis: Programs are to monitor their security controls on an ongoing basis after deployment, including determining the security impact of proposed or actual

[57]Initial remediation should be conducted for vulnerabilities that should be corrected immediately. Remaining vulnerabilities are corrected over time with the use of corrective action plans.

changes to the information system and assessing the security controls in accordance with a monitoring strategy that determines the frequency of monitoring the controls.

For the GMM program's engineering and test environment, which went live in February 2018,[58] FEMA fully addressed three of the five key cybersecurity practices in NIST's risk management framework and partially addressed two of the practices. Specifically, FEMA categorized GMM's environment based on security risk, implemented select security controls, and monitored security controls on an ongoing basis. However, the agency partially addressed the areas of assessing security controls and obtaining an authorization to operate the system. Table 5 provides a summary of the extent to which FEMA addressed NIST's key cybersecurity practices for GMM's engineering and test environment.

Table 5: Extent to Which the Federal Emergency Management Agency Addressed Key Cybersecurity Practices for the Grants Management Modernization Program

Key practice	Overall area rating
Categorize the system based on security risk	Fully addressed
Select and implement security controls	Fully addressed
Assess security controls	Partially addressed
Obtain an authorization to operate the system	Partially addressed
Monitor security controls on an ongoing basis	Fully addressed

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

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

GMM Categorized the System Based on Security Risk

Consistent with NIST's framework, GMM categorized the security risk of its engineering and test environment and identified it as a moderate-impact environment. A moderate-impact environment is one where the loss of confidentiality, integrity, or availability could be expected to have a serious or adverse effect on organizational operations, organizational assets, or individuals. GMM completed the following steps leading to this categorization:

[58]The program's engineering and test environment was intended to mirror the production environment's configuration and security controls. GMM conducted a separate authorization to operate process for the production environment, which went live in July 2018.

- The program documented in its System Security Plan the various types of data and information that the environment will collect, process, and store, such as conducting technology research, building or enhancing technology, and maintaining IT networks.
- The program established three information types and assigned security levels of low, moderate, or high impact in the areas of confidentiality, availability, and integrity. A low-impact security level was assigned to two information types: (1) conducting technology research and (2) building or enhancing technology; and a moderate-impact security level was assigned to the third information type: maintaining IT networks.
- The engineering and test environment was categorized as an overall moderate-impact system, based on the highest security impact level assignment.
- GMM documented a description of the environment, including a diagram depicting the system's boundaries, which illustrates, among other things, databases and firewalls.
- GMM properly registered its engineering and test environment with FEMA's Chief Information Officer, Chief Financial Officer, and acting Chief Information Security Officer.

By conducting the security categorization process, GMM has taken steps that should ensure that the appropriate security controls are selected for the program's engineering and test environment.

GMM Selected and Planned for the Implementation of Controls in Its System Security Plan

Consistent with NIST's framework and the system categorization results, GMM appropriately determined which security controls to implement and planned actions for implementing those controls in its System Security Plan for the engineering and test environment. For example, the program utilized NIST guidance to select standard controls for a system categorized with a moderate-impact security level.[59] These control areas include, for example, access controls, risk assessment, incident response, identification and authentication, and configuration management.

[59]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

Further, the program documented its planned actions to implement each control in its System Security Plan. For example, GMM documented that the program plans to implement its Incident Response Testing control by participating in an agency-wide exercise and unannounced vulnerability scans. As another example, GMM documented that the program plans to implement its Contingency Plan Testing control by testing the contingency plan annually, reviewing the test results, and preparing after action reports. By selecting and planning for the implementation of security controls, GMM has taken steps to mitigate its security risks and protect the confidentiality, integrity, and availability of the information system.

GMM Developed a Security Assessment Plan, but It Lacked Essential Details and Approvals

Consistent with NIST's framework, in January 2018, GMM program officials developed a security assessment plan for the engineering and test environment. According to GMM program officials, this plan was reviewed by the security assessment team.

However, the security assessment plan lacked essential details. Specifically, while the plan included the general process for evaluating the environment's security controls, the planned assessment procedures for all 964 security controls were not sufficiently defined. Specifically, GMM program officials copied example assessment procedures from NIST guidance and inserted them into its security assessment documentation for all of its 964 controls, without making further adjustments to explain the steps that should be taken specific to GMM. Table 6 shows an example of a security assessment procedure copied from the NIST guidance that should have been further adjusted for GMM.

Table 6: Example of the Federal Emergency Management Agency's Grants Management Modernization (GMM) Program's Assessment Procedures Compared to the National Institute of Standards and Technology (NIST) Guidance

Security control	NIST assessment procedure	GMM's assessment procedure
	IA-4.1, Identifier Management	IA-4.1, Identifier Management
Examine (the process of analyzing one or more assessment objects to achieve clarification, the results of which are used to support the determination of security and privacy control completeness, and potential for improvement over time):	Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records	Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records.
Interview (the process of conducting discussions with individuals or groups within an organization to achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security and privacy control completeness, and potential for improvement over time):	Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers	Organizational personnel with identifier management responsibilities.

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

In addition, the actual assessment procedures that the GMM assessors used to evaluate the security controls were not documented. Instead, the program only documented whether each control passed or failed each test.

GMM program officials stated that the planned assessment procedures are based on an agency template that was exported from a DHS compliance tool, and that FEMA security officials have been instructed by the DHS OCIO not to tailor or make any adjustments to the template language. However, the assessment procedures outlined in NIST's guidance are to serve as a starting point for organizations preparing their program specific assessments. According to NIST, organizations are expected to select and tailor their assessment procedures for each security control from NIST's list of suggested assessment options (e.g., review, analyze, or inspect policies, procedures, and related documentation options).

DHS OCIO officials stated that, consistent with NIST's guidance, they expect that components will ensure they are in compliance with the minimum standards and will also add details and additional rigor, as appropriate, to tailor the planned security assessment procedures to fit

their unique missions or needs. In November 2018, in response to our audit, DHS OCIO officials stated that they were meeting with FEMA OCIO officials to understand why they did not document the planned and actual assessment procedures performed by the assessors for GMM. Until FEMA ensures that detailed planned evaluation methods and actual evaluation procedures specific to GMM are defined, the program risks assessing security controls incorrectly, having controls that do not work as intended, and producing undesirable outcomes with respect to meeting the security requirements.

In addition, the security assessment plan was not approved by FEMA's OCIO before proceeding with the security assessment. Program officials stated that approval was not required for the security assessment plan prior to the development of the security assessment report. However, NIST guidance states that the purpose of the security assessment plan approval is to establish the appropriate expectations for the security control assessment. By not getting the security assessment plan approved by FEMA's OCIO before security assessment reviews were conducted, GMM risks inconsistencies with the plan and security objectives of the organization.

Finally, consistent with NIST guidance, GMM performed a security assessment in December 2017 of the engineering and test environment's controls, which identified 36 vulnerabilities (23 critical- and high-impact vulnerabilities and 13 medium- and low-impact vulnerabilities). The program also documented these vulnerabilities and associated findings and recommendations in a security assessment report. GMM conducted initial remediation actions (i.e., remediation of vulnerabilities that should be corrected immediately) for 12 of the critical- and high-impact vulnerabilities and a reassessment of those security controls confirmed that they were resolved by January 2018. Remediation of the remaining 11 critical- and high-impact vulnerabilities and 13 medium- and low-impact vulnerabilities were to be addressed by corrective action plans as part of the authorization to operate process, which is discussed in the next section.

GMM Obtained Authorization to Operate, but Had Not Addressed Known Vulnerabilities or Tested All Controls

The authorization to operate GMM's engineering and test environment was granted on February 5, 2018. Among other things, this decision was based on the important stipulation that the remaining 11 critical- and high-

impact vulnerabilities associated with multifactor authentication would be addressed within 45 days, or by March 22, 2018. However, the program did not meet this deadline and, instead, approximately 2 months after this deadline passed, obtained a waiver to remediate these vulnerabilities by May 9, 2019.

These vulnerabilities are related to a multifactor authentication capability.[60] Program officials stated that they worked with FEMA OCIO officials to attempt to address these vulnerabilities by the initial deadline, but they were unsuccessful in finding a viable solution. Therefore, GMM program officials developed a waiver at the recommendation of the OCIO to provide additional time to develop a viable solution. However, a multifactor authentication capability is essential to ensuring that users are who they say they are, prior to granting users access to the GMM engineering and test environment, in order to reduce the risk of harmful actors accessing the system.

In addition, as of September 2018, the program had not established corrective action plans for the 13 medium- and low-impact vulnerabilities. Program officials stated that they do not typically address low-impact vulnerabilities; however, this is in conflict with DHS guidance that specifies that corrective action plans must be developed for every weakness identified during a security control assessment and within a security assessment report. In response to our audit, in October 2018, GMM program officials developed these remaining corrective action plans. The plans indicated that these vulnerabilities were to be fully addressed by January 2019 and April 2019.

While the program eventually took corrective actions in response to our audit by developing the missing plans, the GMM program initially failed to follow DHS's guidance on preparing corrective actions plans for all security vulnerabilities. Until GMM consistently follows DHS's guidance, it will be difficult for FEMA to determine the extent to which GMM's security weaknesses identified during its security control assessments are remediated. Additionally, as we have reported at other agencies, vulnerabilities can be indicators of more significant underlying issues and, thus, without appropriate management attention or prompt remediation,

[60]The purpose of multifactor authentication is to make it more difficult for an unauthorized person to access a computer system by putting in place several factors of defense. The factors are defined as: (1) something you know (e.g., password), (2) something you have (e.g., token), or (3) something you are (e.g., biometric).

GMM is at risk of unnecessarily exposing the program to potential exploits.[61]

Moreover, GMM was required to assess all untested controls by March 7, 2018, or no later than 30 days after the approval of the authorization to operate; however, it did not meet this deadline. Specifically, we found that, by October 2018, FEMA had not fully tested 190 security controls in the GMM engineering and test environment. These controls were related to areas such as security incident handling and allocation of resources required to protect an information system. In response to our findings, in October 2018, GMM program officials reported that they had since fully tested 27 controls and partially tested the remaining 163 controls.

Program officials stated that testing of the 163 controls is a shared responsibility between GMM and other parties (e.g., the cloud service provider). They added that GMM had completed its portion of the testing but was in the process of verifying the completion of testing by other parties. Program officials stated that the untested controls were not addressed sooner, in part, because of errors resulting from configuration changes in the program's compliance tool during a system upgrade, which have now been resolved. Until GMM ensures that all security controls have been tested, it remains at an increased risk of exposing programs to potential exploits.

GMM Is Using Processes for Monitoring Controls

Consistent with the NIST framework, GMM established methods for assessing and monitoring security controls to be conducted after an authorization to operate has been approved. GMM has tailored its cybersecurity policies and practices for monitoring its controls to take into account the frequent and iterative pace with which system functionality is continuously being introduced into the GMM environment.

Specifically, the GMM program established a process for assessing security impact changes to the system and conducting reauthorizations to operate within the rapid Agile delivery environment. As part of this process, GMM embedded cybersecurity experts on each Agile development team so that they are involved early and can impact security

[61]GAO, *Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement,* GAO-18-210 (Washington, D.C.: Mar. 6, 2018).

considerations from the beginning of requirements development through testing and deployment of system functionality.

In addition, the process involves important steps for ensuring that the system moves from development to completion, while producing a secure and reliable system. For example, it includes procedures for creating, reviewing, and testing new system functionality. As the new system functionality is integrated with existing system functionality, it is to undergo automated testing and security scans in order to ensure that the integrity of the security of the system has not been compromised. Further, an automated process is to deploy the code if it passes all security scans, code tests, and code quality checks.

GMM's process for conducting a reauthorization to operate within the rapid delivery Agile development environment is to follow FEMA guidance that states that all high-level changes made to a FEMA IT system must receive approval from both a change advisory board and the FEMA Chief Information Officer. The board and FEMA Chief Information Officer are to focus their review and approval on scheduled releases and epics (i.e., collections of user stories). Additionally, the Information System Security Officer is to review each planned user story and, if it is determined that the proposed changes may impact the integrity of the authorization, the Information System Security Officer is to work with the development team to begin the process of updating the system authorization.

Finally, GMM uses automated tools to track the frequency in which security controls are assessed and to ensure that required scanning data are received by FEMA for reporting purposes. Program officials stated that, in the absence of department-level and agency-level guidance, they have coordinated with DHS and FEMA OCIO officials to ensure that these officials are in agreement with GMM's approach to continuous monitoring. By having monitoring control policies and procedures in place, FEMA management is positioned to more effectively prioritize and plan its risk response to current threats and vulnerabilities for the GMM program.

Conclusions

Given FEMA's highly complex grants management environment, with its many stakeholders, IT systems, and internal and external users, implementing leading practices for business process reengineering and IT requirements management is critical for success. FEMA has taken many positive steps, including ensuring executive leadership support for

business process reengineering, documenting the agency's grants management processes and performance improvement goals, defining initial IT requirements for the program, incorporating input from end user stakeholders into the development and implementation process, and taking recent actions to improve its delivery of planned IT requirements. Nevertheless, until the GMM program finalizes plans and time frames for implementing its organizational change management actions, plans and communicates system transition activities, and maintains clear traceability of IT requirements, FEMA will be limited in its ability to provide streamlined grants management processes and effectively deliver a modernized IT system to meet the needs of its large range of users.

While GMM's initial cost estimate was reliable, key assumptions about the program since the initial estimate had changed and, therefore, it no longer reflected the current approach for the program. The forthcoming updated cost schedule is expected to better reflect the current approach. However, the program's unreliable schedule to fully deliver GMM by September 2020 is aggressive and unrealistic. The delays the program has experienced to date further compound GMM's schedule issues. Without a robust schedule that has been informed by a realistic assessment of GMM's development activities, leadership will be limited in its ability to make informed decisions on what additional increases in cost or reductions in scope might be needed to achieve their goals.

Further, FEMA's implementation of cybersecurity practices for GMM in the areas of system categorization, selection and implementation, and monitoring will help the program. However, GMM lacked essential details for evaluating security controls, did not approve the security assessment plan before proceeding with the security assessment, did not follow DHS's guidance to develop corrective action plans for all security vulnerabilities, and did not fully test all security controls. As a result, the GMM engineering and test environment remains at an increased risk of exploitations.

Recommendations for Executive Action

We are making eight recommendations to FEMA:

The FEMA Administrator should ensure that the GMM program management office finalizes the organizational change management plan and time frames for implementing change management actions. (Recommendation 1)

The FEMA Administrator should ensure that the GMM program management office plans and communicates its detailed transition activities to its affected customers before they transition to GMM and undergo significant changes to their processes. (Recommendation 2)

The FEMA Administrator should ensure that the GMM program management office implements its planned changes to its processes for documenting requirements for future increments and ensures it maintains traceability among key IT requirements documents. (Recommendation 3)

The FEMA Administrator should ensure that the GMM program management office updates the program schedule to address the leading practices for a reliable schedule identified in this report. (Recommendation 4)

The FEMA Administrator should ensure that the FEMA OCIO defines sufficiently detailed planned evaluation methods and actual evaluation methods for assessing security controls. (Recommendation 5)

The FEMA Administrator should ensure that the FEMA OCIO approves a security assessment plan before security assessment reviews are conducted. (Recommendation 6)

The FEMA Administrator should ensure that the GMM program management office follows DHS guidance on preparing corrective action plans for all security vulnerabilities. (Recommendation 7)

The FEMA Administrator should ensure that the GMM program management office fully tests all of its security controls for the system. (Recommendation 8)

Agency Comments and Our Evaluation

DHS provided written comments on a draft of this report, which are reprinted in appendix IV. In its comments, the department concurred with all eight of our recommendations and provided estimated completion dates for implementing each of them.

For example, with regard to recommendation 4, the department stated that FEMA plans to update the GMM program schedule to address the leading practices for a reliable schedule by April 30, 2019. In addition, for recommendation 7, the department stated that FEMA plans to ensure that

corrective action plans are prepared by July 31, 2019, to address all identified security vulnerabilities for GMM. If implemented effectively, the actions that FEMA plans to take in response to the recommendations should address the weaknesses we identified.

We also received technical comments from DHS and FEMA officials, which we incorporated, as appropriate.

We are sending copies of this report to the Secretary of Homeland Security and interested congressional committees. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-4456 or harriscc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Sincerely yours,

Carol C. Harris
Director, Information Technology Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine the extent to which the Federal Emergency Management Agency (FEMA) is implementing leading practices for reengineering its grants management business processes and incorporating business needs into Grants Management Modernization (GMM) information technology (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 for GMM.

To address the first objective, we reviewed GAO's Business Process Reengineering Assessment Guide[1] and Software Engineering Institute's Capability Maturity Model for Integration for Development[2] to identify practices associated with business process reengineering and IT requirements management. We then selected six areas that, in our professional judgment, represented foundational practices that were of particular importance to the successful implementation of an IT modernization effort that is using Agile development processes. We also selected the practices that were most relevant based on where GMM was in the system development lifecycle and we discussed the practice areas with FEMA officials. The practices are:

- Ensuring executive leadership support for process reengineering
- Assessing the current and target business environment and business performance goals
- Establishing plans for implementing new business processes
- Establishing clear, prioritized, and traceable IT requirements
- Tracking progress in delivering IT requirements
- Incorporating input from end user stakeholders

[1]GAO, *Business Process Reengineering Assessment Guide*—Version 3, GAO/AIMD-10.1.15 (Washington, D.C.: May 1997).

[2]Software Engineering Institute, *Capability Maturity Model® Integration for Development*, Version 1.3 (Pittsburgh, Pa.: November 2010).

We also reviewed selected chapters of GAO's draft Agile Assessment Guide (Version 6A), which is intended to establish a consistent framework based on best practices that can be used across the federal government for developing, implementing, managing, and evaluating agencies' IT investments that rely on Agile methods. To develop this guide, GAO worked closely with Agile experts in the public and private sector; some chapters of the guide are considered more mature because they have been reviewed by the expert panel. We reviewed these chapters to ensure that our expectations for how FEMA should apply the six practices for business process reengineering and IT requirements management are appropriate for an Agile program and are consistent with the draft guidance that is under development. Additionally, since Agile development programs may use different terminology to describe their software development processes, the Agile terms used in this report (e.g., increment, sprint, epic, etc.) are specific to the GMM program.

We obtained and analyzed FEMA grants management modernization documentation, such as current and target grants management business processes, acquisition program baseline, operational requirements document, concept of operations, requirements analyses workbooks, Grants Management Executive Steering Group artifacts, stakeholder outreach artifacts, Agile increment- and sprint-level planning and development artifacts, and the requirements backlog.[3]

We assessed the program documentation against the selected practices to determine the extent to which the agency had implemented them. We then assessed each practice area as:

- fully implemented—FEMA provided complete evidence that showed it fully implemented the practice area;
- partially implemented—FEMA provided evidence that showed it partially implemented the practice area;
- not implemented—FEMA did not provide evidence that showed it implemented any of the practice area.

Additionally, we observed Agile increment and sprint development activities at GMM facilities in Washington, D.C. We also observed a

[3]Since GMM uses Agile software development, which allows for specific plans and IT requirements to be defined on an incremental basis, we focused on GMM's plans and requirements for near-term efforts, which consisted of Increment 1 (i.e., the Assistance to Firefighters Grants Pilot).

demonstration of how the program manages its lower level requirements (i.e., user stories and epics) and maintains traceability of the requirements using an automated tool at GMM facilities in Washington, D.C.

We also interviewed FEMA officials, including the GMM Program Executive, GMM Program Manager, GMM Business Transformation Team Lead, and Product Owner regarding their efforts to streamline grants management business processes, collect and incorporate stakeholder input, and manage GMM's requirements. In addition, we interviewed FEMA officials from four out of 16 grant program offices and two out of 10 regional offices to obtain contextual information and illustrative examples of FEMA's efforts to reengineer grants management business processes and collect business requirements for GMM. Specifically,

- We selected the four grant program offices based on a range of grant programs managed, legacy systems used, and the amount of grant funding awarded. We also sought to select a cross section of different characteristics, such as selecting larger grant program offices, as well as smaller offices. In addition, we ensured that our selection included the Assistance to Firefighters Grants (AFG) program office because officials in this office represent the first GMM users and, therefore, are more actively involved with the program's Agile development practices. Based on these factors, we selected: Public Assistance Division, Individual Assistance Division, AFG, and National Fire Academy. Additionally, the four selected grant program offices are responsible for 16 of the total 45 grant programs and are users of five of the nine primary legacy IT systems. The four selected grant program offices also represent about 68 percent of the total grant funding awarded by FEMA from fiscal years 2005 through 2016.
- We selected two regional offices based on (1) the largest amount of total FEMA grant funding for fiscal years 2005 through 2016—Region 6 located in Denton, Texas; and (2) the highest percentage of AFG funding compared to the office's total grant funding awarded from fiscal years 2005 through 2016—Region 5 located in Chicago, Illinois.

To assess the reliability of data from the program's automated IT requirements management tool, we interviewed knowledgeable officials about the quality control procedures used by the program to assure accuracy and completeness of the data. We also compared the data to other relevant program documentation on GMM requirements. We

determined that the data used were sufficiently reliable for the purpose of evaluating GMM's practices for managing IT requirements.

For our second objective, to assess the reliability of GMM's estimated costs and schedule, we reviewed documentation on GMM's May 2017 lifecycle cost estimate and on the program's schedule, dated May 2018.

- To assess the reliability of the May 2017 lifecycle cost estimate, we evaluated documentation supporting the estimate, such as the cost estimating model, the report on GMM's Cost Estimating Baseline Document and Life Cycle Cost Estimate, and briefings provided to the Department of Homeland Security (DHS) and FEMA management regarding the cost estimate. We assessed the cost estimating methodologies, assumptions, and results against leading practices for developing a comprehensive, accurate, well-documented, and credible cost estimate, identified in GAO's Cost Estimating and Assessment Guide.[4] We also interviewed program officials responsible for developing and reviewing the cost estimate to understand their methodology, data, and approach for developing the estimate. We found that the cost data were sufficiently reliable.
- To assess the reliability of the May 2018 GMM program schedule, we evaluated documentation supporting the schedule, such as the integrated master schedule, acquisition program baseline, and Agile artifacts.[5] We assessed the schedule documentation against leading practices for developing a comprehensive, well-constructed, credible, and controlled schedule, identified in GAO's Schedule Assessment Guide.[6] We also interviewed GMM program officials responsible for developing and managing the program schedule to understand their practices for creating and maintaining the schedule. We noted in our report the instances where the quality of the schedule data impacted the reliability of the program's schedule.

[4]GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs,* GAO-09-3SP (Washington, D.C.: March 2009).

[5]Since GMM uses Agile software development, which allows for high level plans to be defined in further detail on an incremental basis, we focused on GMM's near-term planning efforts which consisted of Increment 1 (i.e., the Assistance to Firefights Grants Pilot).

[6]GAO, *Schedule Assessment Guide: Best Practices for Project Schedules,* GAO-16-89G (Washington, D.C.: December 2015).

For both the cost estimate and program schedule, we assessed each leading practice as:

- fully addressed—FEMA provided complete evidence that showed it implemented the entire practice area;
- substantially addressed—FEMA provided evidence that showed it implemented more than half of the practice area;
- partially addressed—FEMA provided evidence that showed it implemented about half of the practice area;
- minimally addressed—FEMA provided evidence that showed it implemented less than half of the practice area;
- not addressed—FEMA did not provide evidence that showed it implemented any of the practice area.

Finally, we provided FEMA with draft versions of our detailed analyses of the GMM cost estimate and schedule. This was done to verify that the information on which we based our findings was complete, accurate, and up-to-date.

Regarding our third objective, to determine the extent to which FEMA is addressing key cybersecurity practices for GMM, we reviewed documentation regarding DHS and FEMA cybersecurity policies and guidance, and FEMA's authorization to operate for the program's engineering and test environment.[7] We evaluated the documentation against all six cybersecurity practices identified in the National Institute of Standards and Technology's (NIST) Risk Management Framework.[8] While NIST's Risk Management Framework identifies six total practices, for reporting purposes, we combined two interrelated practices—selection of security controls and implementation of security controls—into a single practice. The resulting five practices were: categorizing the system based on security risk, selecting and implementing security controls, assessing

[7]The programs' engineering and test environment went live in February 2018 and was the most recent authorization to operate at the time that we began our review. This environment was intended to mirror the production environment's configuration and security controls. GMM subsequently conducted a separate authorization to operate process for the production environment, which went live in July 2018.

[8]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

security controls, obtaining an authorization to operate the system, and monitoring security controls on an ongoing basis.

We obtained and analyzed key artifacts supporting the program's efforts to address these risk management practices, including the program's System Security Plan, the Security Assessment Plan and Report, Authorization to Operate documentation, and the program's continuous monitoring documentation. We also interviewed officials from the GMM program office and FEMA's Office of the Chief Information Officer, such as the GMM Security Engineering Lead, GMM Information System Security Officer, and FEMA's Acting Chief Information Security Officer, regarding their efforts to assess, document, and review security controls for GMM. We assessed the evidence against the five practices to determine the extent to which the agency had addressed them. We then assessed each practice area as:

- fully addressed—FEMA provided complete evidence that showed it fully implemented the practice area;
- partially addressed—FEMA provided evidence that showed it partially implemented the practice area;
- not addressed—FEMA did not provide evidence that showed it implemented any of the practice area.

To assess the reliability of data from the program's automated security controls management tool, we interviewed knowledgeable officials about the quality control procedures used by the program to assure accuracy and completeness of the data. We also compared the data to other relevant program documentation on GMM security controls for the engineering and test environment. We found that some of the security controls data we examined were sufficiently reliable for the purpose of evaluating FEMA's cybersecurity practices for GMM, and we noted in our report the instances where the accuracy of the data impacted the program's ability to address key cybersecurity practices.

We conducted this performance audit from December 2017 to April 2019 in accordance with 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Federal Emergency Management Agency's Grant Programs

The Federal Emergency Management Agency (FEMA) awards many different types of grants to state, local, and tribal governments and nongovernmental entities. These grants are to help communities prevent, prepare for, protect against, mitigate the effects of, respond to, and recover from disasters and terrorist attacks.

The number of active grant programs varies based on programs being authorized or discontinued and how "grant programs" are defined. In 2018, FEMA Office of Chief Counsel officials identified 37 programs, whereas Grants Management Modernization (GMM) program officials identified 45 programs because they defined "grant programs" more broadly and further decomposed the programs to facilitate the development of the GMM solution. The following 45 active grant programs were identified by GMM, as of August 2018:

1. Assistance to Firefighters Grants
2. Chemical Stockpile Emergency Preparedness Program
3. Community Assistance Program - State Support Services Element
4. Complex Coordinated Terrorist Attacks Program
5. Cooperating Technical Partners
6. Cora Brown Fund
7. Countering Violent Extremism
8. Crisis Counseling Program
9. Disaster Case Management Grants
10. Disaster Housing Operations for Individuals and Households
11. Disaster Legal Services
12. Disaster Unemployment Assistance
13. Emergency Food and Shelter National Board Program

14. Emergency Management Baseline Assessments Grant
15. Emergency Management Institute Training Assistance
16. Emergency Management Performance Grants
17. Fire Management Assistance Grant
18. Fire Prevention and Safety Grants
19. Flood Mitigation Assistance
20. Hazard Mitigation Grant Program
21. Homeland Security Grant Program: Operation Stonegarden Grant Program
22. Homeland Security Grant Program: State Homeland Security Program
23. Homeland Security Grant Program: Urban Areas Security Initiative
24. Homeland Security National Training Program/National Domestic Preparedness Consortium
25. Homeland Security National Training Program/Continuing Training Grant
26. Homeland Security Preparedness Technical Assistance Program
27. Housing Assistance
28. Intercity Bus Security Grant Program
29. Intercity Passenger Rail Program
30. National Dam Safety Program
31. National Earthquake Hazard Reduction Program
32. National Fire Academy Training Assistance
33. National Incident Management System – Emergency Management Assistance Compact
34. Nonprofit Security Grant Program
35. Other Needs Assistance
36. Port Security Grant Program
37. Pre-Disaster Mitigation
38. Presidential Residence Protection Assistance
39. Public Assistance
40. Staffing for Adequate Fire and Emergency Response Grants

41. State Fire Training System Grant
42. Transit Security Grant Program
43. Tribal Homeland Security Grant Program
44. Urban Search and Rescue Readiness Cooperative Agreements
45. Urban Search and Rescue Response Cooperative Agreements

Appendix III: Overview of Agile Software Development

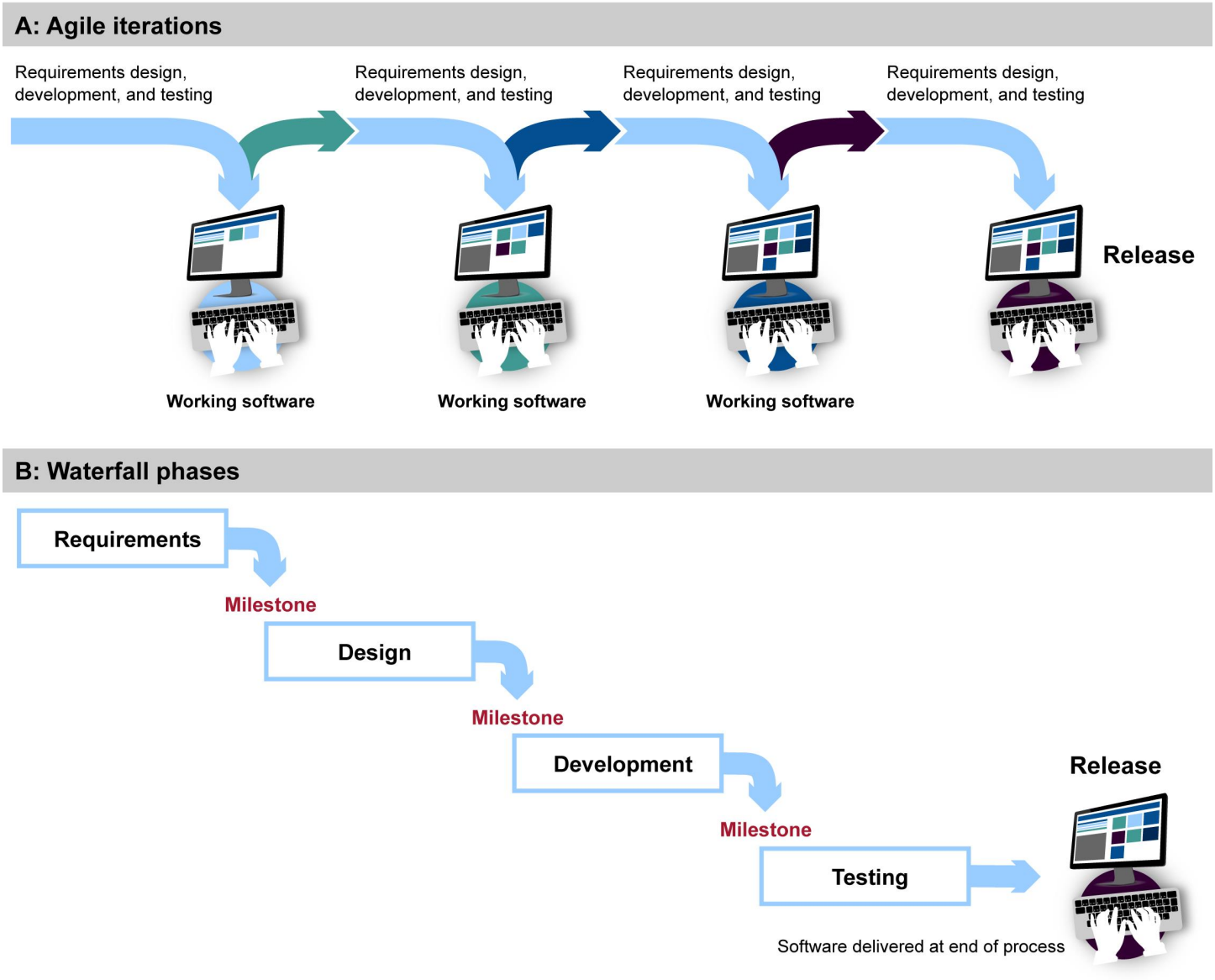
Agile software development is a type of incremental development that calls for the rapid delivery of software in small, short increments. The use of an incremental approach is consistent with the Office of Management and Budget's guidance as specified in its information technology (IT) Reform Plan,[1] as well as the legislation commonly referred to as the Federal Information Technology Acquisition Reform Act.[2]

Many organizations, especially in the federal government, are accustomed to using a waterfall software development model, which typically consists of long, sequential phases, and differs significantly from the Agile development approach. Agile practices integrate planning, design, development, and testing into an iterative lifecycle to deliver software early and often. Figure 7 provides a depiction of software development using the Agile approach, as compared to a waterfall approach.

[1]Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010). The implementation plan states that funding of major IT programs should only be approved when it uses a modular approach with usable functionality delivered every 6 months.

[2]40 U.S.C. § 11319(b)(1)(B)(ii). The Federal Information Technology Acquisition Reform provisions of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014) are commonly referred to as the Federal Information Technology Acquisition Reform Act. The act directs the Office of Management and Budget to require in its annual capital planning guidance that the chief information officers of covered agencies certify that IT investments are adequately implementing incremental development. The Office of Management and Budget defines adequate incremental development of software or services as the delivery of new or modified technical functionality to users at least every 6 months.

Figure 7: Comparison of Agile and Waterfall Software Development



Source: GAO. | GAO-19-164

The frequent iterations of Agile development are intended to effectively measure progress, reduce technical and programmatic risk, and respond to feedback from stakeholders in changes to IT requirements more quickly than traditional methods. Despite these intended benefits,

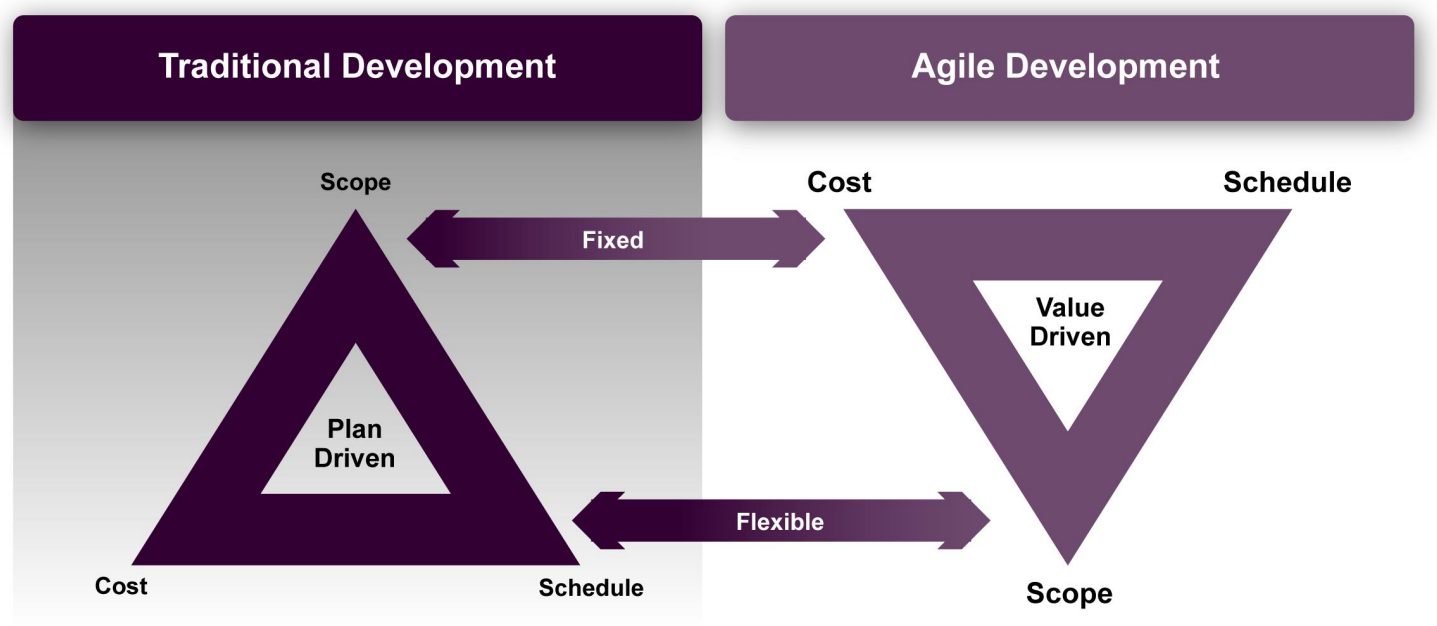
organizations adopting Agile must overcome challenges in making significant changes to how they are accustomed to developing software.[3]

The significant differences between Agile and waterfall development impact how IT programs are planned, implemented, and monitored in terms of cost, schedule, and scope. For example, in waterfall development, significant effort is devoted upfront to document detailed plans and all IT requirements for the entire scope of work at the beginning of the program, and cost and schedule can be varied to complete that work.

However, for Agile programs the precise details are unknown upfront, so initial planning of cost, scope, and timing would be conducted at a high level, and then supplemented with more specific plans for each iteration. While cost and schedule are set for each iteration, requirements for each iteration (or increment) can be variable as they are learned over time and revised to reflect experiences from completed iterations and to accommodate changing priorities of the end users. The differences in these two software development approaches are shown in figure 8.

[3]See prior reports highlighting challenges with adopting Agile practices, such as GAO, *Software Development: Effective Practices and Federal Challenges in Applying Agile Methods,* GAO-12-681 (Washington, D.C.: July 27, 2012); *Immigration Benefits System: U.S. Citizenship and Immigration Services Can Improve Program Management,* GAO-16-467 (Washington, D.C.: July 7, 2016); and *TSA Modernization: Use of Sound Program Management and Oversight Practices Is Needed to Avoid Repeating Past Problems,* GAO-18-46 (Washington, D.C.: Oct. 17, 2017).

Figure 8: Comparison of Cost, Schedule, and Scope Management for Each Iteration among Software Development Approaches



Source: GAO. | GAO-19-164

Looking at figure 8, the benefit provided from using traditional program management practices such as establishing a cost estimate or a robust schedule, is not obvious. However, unlike a theoretical environment, many government programs may not have the autonomy to manage completely flexible scope, as they must deliver certain minimal specifications with the cost and schedule provided. In those cases, it is vital for the team to understand and differentiate the IT requirements that are “must haves” from the “nice to haves” early in the planning effort. This would help facilitate delivery of the “must-haves” requirements first, thereby providing users with the greatest benefits as soon as possible.

Appendix IV: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

March 18, 2019

Carol C. Harris
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-164, "FEMA GRANTS MODERNIZATION: Improvements Needed to Strengthen Program Management and Cybersecurity"

Dear Ms. Harris:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of the many positive steps the Federal Emergency Management Agency (FEMA) has taken to implement leading practices for effective business process reengineering and information technology (IT) requirements. These include ensuring executive leadership support for business process reengineering and incorporating input from end user stakeholders. DHS and FEMA are committed to the successful implementation of the Grants Management Modernization (GMM) program, which aims to transform the way FEMA manages grants, strengthening FEMA's ability to execute its mission through a user-centered, business-driven approach.

The draft report contained eight recommendations with which the Department 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.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

2

Attachment: Management Response to Recommendations Contained in GAO-19-164

GAO recommended that the FEMA Administrator:

Recommendation 1: Ensure that the GMM Program management office finalizes the organizational change management plan and time frames for implementing change management actions.

Response: Concur. The GMM Program Management Office (PMO) will ensure the change management efforts are further developed and implemented with the various grants programs in the Agency.

The GMM PMO has identified key resources to focus on maturing its change management efforts. These key resources include the GMM Business Manager, Regional Coordinator, Change Manager, Training Manager, and a Business Analyst who will partner with the various grant programs and champion GMM's change management across the agency. GMM will first update its Change Management Plan (CMP) to add additional details, where available, to include organizational change, workforce impacts, and readiness. GMM is currently reviewing its CMP and will develop a Plan of Action & Milestones (POAM) by July 31, 2019 to guide the program and establish timeframes for implementation. In the Change Management POAM, GMM will identify target dates to create an Organizational Change Management Strategy, Readiness Assessment, Training Plan, and Workforce Analysis. The development of these documents will support the overall implementation of change management efforts in GMM with users from all grant programs.

In addition to supporting organizational change management, GMM has helped stand up the Centralized Grants Policy & Doctrine Working Group (CWG) to identify opportunities for standardizing grant policies and/or processes in order to ensure alignment with the FEMA Manual 205-0-1, "Grants Management," as well as ensuring accurate and qualitative buildouts of the GMM system (aka FEMA GO). The CWG is a cross-Agency team of policy experts from the various grant programs. The initial phase of the team's efforts will be focused on resolving policy and process questions that arise during the development of the FEMA GO system that are beyond what is addressed in the Grants Management Manual. Decisions made by this team will be captured in updates to the Grants Management Manual, supporting standard operating procedures, and incorporated in the updated CMP.

Estimated Completion Date (ECD): July 31, 2020.

3

Recommendation 2: Ensure that the GMM program management office plans and communicates its detailed transition activities to its affected customers before they transition to GMM and undergo significant changes to their processes.

Response: Concur. The GMM PMO will ensure a detailed transition of activities for users to optimally manage significant changes to their current business processes. The GMM PMO will conduct a readiness assessment to better understand our users and their ability to undergo significant changes to their grants business processes, per the timeline identified in the CMP POAM. The assessment will analyze how prepared and ready FEMA users are to use new functionality in FEMA GO, review how users are trained with current grants management and how much training is needed to support the transition to the FEMA GO system, identify areas needing more attention for users, and make recommendations that significantly increase the likelihood of GMM success and FEMA GO user adoption. The initial transition plan to support the Assistance to Firefighters Grants pilot will be completed by August 31, 2019.

ECD: December 31, 2019.

Recommendation 3: Ensure that the GMM program management office implements its planned changes to its processes for documenting requirements for future increments and ensures it maintains traceability among key IT requirements documents.

Response: Concur. GMM is leveraging industry best practices while implementing Agile and Kanban software development methodologies. The GMM team is documenting the Jira Software product backlog, which provides complete traceability through acceptance criteria and gets mapped to test plans and test cases. GMM will provide mapping of functions to the Jira backlog to ensure complete end-to-end traceability. Jira is the DHS software suite used by GMM to manage Agile software requirements and measure development progress.

ECD: July 31, 2019.

Recommendation 4: Ensure that the GMM program management office updates the program schedule to address the leading practices for a reliable schedule identified in this report.

Response: Concur. GMM Program leadership will ensure that the GMM PMO updates the program schedule to address the leading practices for a reliable schedule identified in this report.

In October 2018, the program added two master schedulers to the PMO team to work on the GMM Program Integrated Master Schedule (IMS). In addition, the program detailed a dedicated portfolio manager to begin building a program level Release Plan that

4

incorporates product requirements across all FEMA lines of business and illustrates software development goals, objectives, and milestones for when features (new functionality) will be delivered to users.

The program level Release Plan will be further revised with input from the Systems and Platform using Agile Releases and Consolidation (SPARC) software development contractor. The initial planning task awarded to the SPARC contractor includes a requirement to develop a "comprehensive Integrated Master Schedule (IMS) that incorporates all projects, activities, and milestones necessary for the design, development, and implementation of the GMM target solution."

ECD: April 30, 2019.

Recommendation 5: Ensure that the FEMA OCIO defines sufficiently detailed planned evaluation methods and actual evaluation methods for assessing security controls.

Response: Concur. FEMA's Office of the Chief Information Officer (OCIO) Cyber Security Division (CSD) will plan and conduct security control evaluations as annotated in the Cybersecurity Security Assessment Plan Standard Operating Procedures. The CSD Security Control Assessor will work with the GMM program Information Systems Security Officer to ensure security controls are implemented and documented in the Security Assessment Report with sufficient detail to meet DHS Sensitive Policy Systems Directive 4300A and National Institute of Standards and Technology (NIST) 800-53 mandates.

ECD: July 31, 2019.

Recommendation 6: Ensure that the FEMA OCIO approves a security assessment plan before security assessment reviews are conducted.

Response: Concur. FEMA OCIO CSD will document and implement processes and procedures in accordance with NIST SP 800-37, "Guidelines for Applying the Risk Management Framework to Federal Information Systems," and "DHS Sensitive Policy Systems Directive 4300A," for the Security Control Assessor to review and validate in the Security Assessment Plan. The GMM system owner and independent verification and validation team lead will approve and sign the required Scanning Authorization Letter included in the Security Assessment Plan prior to conducting any system security assessments. This will grant Security Control Assessors the authority to scan and assess the system.

ECD: July 31, 2019.

Recommendation 7: Ensure that the GMM Program management office follows DHS guidance on preparing corrective action plans for all security vulnerabilities.

Response: Concur. The GMM Program will expand its corrective action plans to comply with mandated guidance for corrective Plans of Action and Milestones to detail remediation of identified vulnerabilities. These guidelines will be compliant with DHS Instruction 4300A, Attachment-H (Plan of Action and Milestones).

On August 17, 2018, FEMA OCIO established a formal Agile Development, Security, and Operations (DevSecOps) process that allows the GMM program to securely deploy new software into a production environment in a true Agile process. This allows software deployments to occur in minutes/hours compared to days/weeks in a traditional waterfall-based software development process.

GMM is continuing to use automated DevSecOps pipelines and security tools to identify security vulnerabilities. This allows early identification and remediation as quickly as possible. The program has adopted security best practices as part of the overall delivery lifecycle. GMM is leveraging dynamic & static security scans which identifies code vulnerabilities as part of the DevSecOps deployment process. This step prevents any code vulnerabilities being introduced and provides a remediation path for course correction. The environment also undergoes periodic network scans to identify any security vulnerabilities which get patched on a regular basis. The platform is hosted on an accredited cloud infrastructure on a cloud architecture which is patched on a daily basis to address any zero-day vulnerability attack vector. GMM has also implemented additional defense-in-depth features to prevent against malicious attacks. During December 2018, GMM invited DHS cybersecurity professionals to conduct an exhaustive vulnerability assessment of the FEMA GO system, which were unable to identify any vulnerabilities. The scan results provided a good validation of the program's strong security posture.

ECD: July 31, 2019.

Recommendation 8: Ensure that the GMM Program management office fully tests all of its security controls for the system.

Response: Concur. The GMM Program Office will work with FEMA OCIO to ensure a detailed evaluation of all DHS and NIST security controls are annotated in the Security Assessment Plan. OCIO CSD Security Control Assessors will work with the GMM system owner and program ISSO to ensure security controls are implemented and documented with sufficient details to meet DHS Directive 4300A and NIST 800-53 mandates, allowing for comprehensive testing of the system.

6

As of October 2018, GMM has worked with CSD to obtain and document all inherited controls and the systems that provide these controls. GMM is working to identify and compile the Points of Contact (POCs) for these systems, (for both DHS and FEMA). GMM will continue to work with these POCs to ensure that all inherited controls are tested by all parties who have a share in the provision of the control and that these are documented in FEMA's Information Assurance Compliance System (IACS). GMM has worked to improve the FEMA GO engineering/test environment documentation in IACS and will continuously do so.

DHS has a well-documented Security Management plan that provides guidance with respect to security management processes such as common controls and ongoing authorization. With the integration of new technology, and best practices such as Information Security Continuous Monitoring, cloud computing, and security control inheritance, the customary ways of addressing these areas of security are gradually transforming.

The GMM Program is planning to leverage a multi-pronged approach to test all of its security controls for the system. This includes the use of:

- automated tools,
- centralized logging tools such as Splunk, and
- periodic manual testing, to detect and alert on deviation from implemented security controls for the system.

ECD: July 31, 2019.

7

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris at (202) 512-4456 or harriscc@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Shannin G. O'Neill (Assistant Director), Jeanne Sung (Analyst in Charge), Andrew Beggs, Rebecca Eyler, Kendrick Johnson, Thomas J. Johnson, Jason Lee, Jennifer Leotta, and Melissa Melvin.

Appendix VI: Accessible Data

Agency Comment Letter

Text of Appendix IV: Comments from the Department of Homeland Security

Page 1

March 18, 2019

Carol C. Harris
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-164, "FEMA GRANTS MODERNIZATION: Improvements Needed to Strengthen Program Management and Cybersecurity"

Dear Ms. Harris:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of the many positive steps the Federal Emergency Management Agency (FEMA) has taken to implement leading practices for effective business process reengineering and information technology (IT) requirements. These include ensuring executive leadership support for business process reengineering and incorporating input from end user stakeholders. DHS and FEMA are committed to the successful implementation of the Grants Management Modernization (GMM) program, which aims to transform the way FEMA manages grants, strengthening FEMA' s ability to execute its mission through a user-centered , business-driven approach.

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

Page 2

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.

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG
Liaison Office

Attachment

Page 3

Attachment: Management Response to Recommendations Contained in GA0-19-164

GAO recommended that the FEMA Administrator:

Recommendation 1:

Ensure that the GMM Program management office finalizes the organizational change management plan and time frames for implementing change management actions. Response: Concur. The GMM Program Management Office (PMO) will ensure the change management efforts are further developed and implemented with the various grants programs in the Agency.

The GMM PMO has identified key resources to focus on maturing its change management efforts. These key resources include the GMM Business Manager, Regional Coordinator, Change Manager, Training Manager, and a Business Analyst who will partner with the various grant programs and champion GMM's change management across the agency. GMM will first update its Change Management Plan (CMP) to add additional details, where available, to include organizational change,

workforce impacts, and readiness. GMM is currently reviewing its CMP and will develop a Plan of Action & Milestones (POAM) by July 31, 2019 to guide the program and establish timeframes for implementation. In the Change Management POAM, GMM will identify target dates to create an Organizational Change Management Strategy, Readiness Assessment, Training Plan, and Workforce Analysis. The development of these documents will support the overall implementation of change management efforts in GMM with users from all grant programs.

In addition to supporting organizational change management, GMM has helped stand up the Centralized Grants Policy & Doctrine Working Group (CWG) to identify opportunities for standardizing grant policies and/or processes in order to ensure alignment with the FEMA Manual 205-0-1, "Grants Management," as well as ensuring accurate and qualitative buildouts of the GMM system (aka FEMA GO). The CWG is a cross-Agency team of policy experts from the various grant programs. The initial phase of the team's efforts will be focused on resolving policy and process questions that arise during the development of the FEMA GO system that are beyond what is addressed in the Grants Management Manual. Decisions made by this team will be captured in updates to the Grants Management Manual, supporting standard operating procedures, and incorporated in the updated CMP.

Estimated Completion Date (ECO): July 31, 2020.

Page 4

Recommendation 2:

Ensure that the GMM program management office plans and communicates its detailed transition activities to its affected customers before they transition to GMM and undergo significant changes to their processes.

Response: Concur. The GMM PMO will ensure a detailed transition of activities for users to optimally manage significant changes to their current business processes. The GMM PMO will conduct a readiness assessment to better understand our users and their ability to undergo significant changes to their grants business processes, per the timeline identified in the CMP POAM. The assessment will analyze how prepared and ready FEMA users are to use new functionality in FEMA GO, review how users are trained with current grants management and how much training is needed to support the transition to the FEMA GO system,

identify areas needing more attention for users, and make recommendations that significantly increase the likelihood of GMM success and FEMA GO user adoption. The initial transition plan to support the Assistance to Firefighters Grants pilot will be completed by August 31, 2019.

ECD: December 31, 2019.

Recommendation 3:

Ensure that the GMM program management office implements its planned changes to its processes for documenting requirements for future increments and ensures it maintains traceability among key IT requirements documents.

Response: Concur. GMM is leveraging industry best practices while implementing Agile and Kanban software development methodologies. The GMM team is documenting the Jira Software product backlog, which provides complete traceability through acceptance criteria and gets mapped to test plans and test cases. GMM will provide mapping of functions to the Jira backlog to ensure complete end-to-end traceability. Jira is the DHS software suite used by GMM to manage Agile software requirements and measure development progress.

ECD: July 31, 2019.

Recommendation 4:

Ensure that the GMM program management office updates the program schedule to address the leading practices for a reliable schedule identified in this report.

Response: Concur. GMM Program leadership will ensure that the GMM PMO updates the program schedule to address the leading practices for a reliable schedule identified in this report.

In October 2018, the program added two master schedulers to the PMO team to work on the GMM Program Integrated Master Schedule (IMS). In addition, the program detailed a dedicated portfolio manager to begin building a program level Release Plan that…

Page 5

…incorporates product requirements across all FEMA lines of business and illustrates software development goals, objectives, and milestones for when features (new functionality) will be delivered to users.

The program level Release Plan will be further revised with input from the Systems and Platform using Agile Releases and Consolidation (SPARC) software development contractor. The initial planning task awarded to the SPARC contractor includes a requirement to develop a "comprehensive Integrated Master Schedule (IMS) that incorporates all projects, activities, and milestones necessary for the design, development and implementation of the GMM target solution."

ECD: April 30, 2019.

Recommendation 5:

Ensure that the FEMA OCIO defines sufficiently detailed planned evaluation methods and actual evaluation methods for assessing security controls.

Response: Concur. FEMA 's Office of the Chief Information Officer (OCIO) Cyber Security Division (CSD) will plan and conduct security control evaluations as annotated in the Cybersecurity Security Assessment Plan Standard Operating Procedures. The CSD Security Control Assessor will work with the GMM program Information Systems Security Officer to ensure security controls are implemented and documented in the Security Assessment Report with sufficient detail to meet DHS Sensitive Policy Systems Directive 4300A and National Institute of Standards and Technology (NIST) 800-53 mandates.

ECO: July 31, 2019.

Recommendation 6:

Ensure that the FEMA OCIO approves a security assessment plan before security assessment reviews are conducted.

Response: Concur. FEMA OCIO CSD will document and implement processes and procedures in accordance with NIST SP 800-37, "Guidelines for Applying the Risk Management Framework to Federal Information Systems," and "DHS Sensitive Policy Systems Directive

4300A," for the Security Control Assessor to review and validate in the Security Assessment Plan. The GMM system owner and independent verification and validation team lead will approve and sign the required Scanning Authorization Letter included in the Security Assessment Plan prior to conducting any system security assessments. This will grant Security Control Assessors the authority to scan and assess the system.

ECD: July 31, 2019.

Page 6

Recommendation 7:

Ensure that the GMM Program management office follows DHS guidance on preparing corrective action plans for all security vulnerabilities.

Response: Concur. The GMM Program will expand its corrective action plans to comply with mandated guidance for corrective Plans of Action and Milestones to detail remediation of identified vulnerabilities. These guidelines will be compliant with DHS Instruction 4300A, Attachment-H (Plan of Action and Milestones).

On August 17, 2018, FEMA OCIO established a formal Agile Development, Security, and Operations (DevSecOps) process that allows the GMM program to securely deploy new software into a production environment in a true Agile process. This allows software deployments to occur in minutes/hours compared to days/weeks in a traditional waterfall-based software development process.

GMM is continuing to use automated DevSecOps pipelines and security tools to identify security vulnerabilities. This allows early identification and remediation as quickly as possible. The program has adopted security best practices as part of the overall delivery lifecycle. GMM is leveraging dynamic & static security scans which identifies code vulnerabilities as part of the DevSecOps deployment process. This step prevents any code vulnerabilities being introduced and provides a remediation path for course correction. The environment also undergoes periodic network scans to identify any security vulnerabilities which get patched on a regular basis. The platform is hosted on an accredited cloud infrastructure on a cloud architecture which is patched on a daily basis to address any zero-day vulnerability attack vector. GMM has also implemented additional defense-in-depth features to prevent against malicious attacks. During December 2018, GMM invited DHS cybersecurity professionals to

conduct an exhaustive vulnerability assessment of the FEMA GO system, which were unable to identify any vulnerabilities. The scan results provided a good validation of the program' s strong security posture.

ECD: July 31, 2019.

Recommendation 8:

Ensure that the GMM Program management office fully tests all of its security controls for the system.

Response: Concur. The GMM Program Office will work with FEMA OCIO to ensure a detailed evaluation of all DHS and NIST security controls are annotated in the Security Assessment Plan. OCIO CSD Security Control Assessors will work with the GMM system owner and program ISSO to ensure security controls are implemented and documented with sufficient details to meet DHS Directive 4300A and NIST 800-53 mandates, allowing for comprehensive testing of the system.

Page 7

As of October 2018, GMM has worked with CSD to obtain and document all inherited controls and the systems that provide these controls. GMM is working to identify and compile the Points of Contact (POCs) for these systems, (for both DHS and FEMA). GMM will continue to work with these POCs to ensure that all inherited controls are tested by all parties who have a share in the provision of the control and that these are documented in FEMA's Information Assurance Compliance System (IACS). GMM has worked to improve the FEMA GO engineering/test environment documentation in IACS and will continuously do so.

DHS has a well-documented Security Management plan that provides guidance with respect to security management processes such as common controls and ongoing authorization. With the integration of new technology, and best practices such as Information Security Continuous Monitoring, cloud computing, and security control inheritance, the customary ways of addressing these areas of security are gradually transforming.

The GMM Program is planning to leverage a multi-pronged approach to test all of its security controls for the system. This includes the use of:

- automated tools,

- centralized logging tools such as Splunk, and
- periodic manual testing, to detect and alert on deviation from implemented security controls for the system.

ECD: July 31, 2019.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548