



February 2022

INFORMATION TECHNOLOGY

OPM Needs to Adopt Key Practices in Modernizing Legacy Financial System

GAO Highlights

Highlights of [GAO-22-104206](#), a report to congressional committees

Why GAO Did This Study

OPM's legacy financial system, FFS, helps manage over \$1 trillion in combined assets and supports over 8 million federal employees and retirees. However, according to OPM, FFS is outdated and consists of unsupported software. In fiscal year 2017, OPM created the Trust Funds Modernization (TFM) Program to replace FFS. In 2019, the agency selected a shared service provider to provide the replacement system.

The House report accompanying the Consolidated Appropriations Act, 2020 included a provision for GAO to examine OPM's effort to modernize and replace FFS. This report (1) describes the status of OPM's effort to modernize and replace FFS; (2) evaluates the progress OPM has made in implementing key modernization practices for using a shared service provider; and (3) determines to what extent the TFM program has adopted leading practices for requirements management, cost and schedule estimation, and cybersecurity. To do so, GAO analyzed relevant TFM program documentation; assessed documentation against key modernization practices; and compared the program's requirements management, cost and schedule estimation, and cybersecurity to leading practices. GAO also interviewed OPM officials.

What GAO Recommends

GAO is making five recommendations to OPM to improve its effort. OPM concurred with two recommendations, partially concurred with two, and did not concur with one. GAO maintains the recommendations as discussed in this report are warranted.

View [GAO-22-104206](#). For more information, contact Kevin Walsh at (202) 512-6151 or walshk@gao.gov.

February 2022

INFORMATION TECHNOLOGY

OPM Needs to Adopt Key Practices in Modernizing Legacy Financial System

What GAO Found

The U.S. Office of Personnel Management (OPM) has completed several phases of its effort to modernize its Trust Funds Federal Financial System (FFS). Among other activities, OPM defined the project's charter, selected a service provider, and gathered requirements. However, as shown below, OPM had to extend the planned completion date of two upcoming milestones by 1 year to October 2022 and October 2023. These milestones focus on the transition to the shared service provider and the new system. In addition, OPM increased the estimated cost of project development and implementation by \$13.4 million to \$71.9 million.

Status of the Office of Personnel Management's (OPM) Financial System Modernization

Phase	Completed or planned completion date
Assessment, Readiness, and Selection	Completed September 2018
Engagement Phase 1	Completed February 2020
Engagement Phase 2	Completed September 2020
Migration Release 1	Planned completion by October 2022 (originally estimated to be completed in October 2021)
Migration Release 2	Planned completion by October 2023 (originally estimated to be completed in October 2022)

Legend:

■ = milestones that have been completed

Source: GAO analysis of OPM's documentation and interviews. | GAO-22-104206

OPM attributed the delay to a variety of reasons, including poor documentation and insufficient staff expertise regarding the legacy system.

OPM partially implemented key practices for using a shared service provider. Specifically, while OPM performed risk assessments of the modernization, the assessments were not comprehensive or did not accurately reflect the risks the program was facing. Specifically, while OPM performed recommended assessments of the modernization, it did not address all known risks. For example, the risk assessment during Engagement Phase 2 did not reflect that OPM had not defined service level agreements for operations and maintenance; applicable guidance considers this omission a high risk at this stage. Further, while OPM conducted recommended reviews at the conclusion of each phase, in two cases the agency moved forward on the modernization without meeting defined exit criteria.

In addition, while OPM fully adopted leading information technology (IT) management practices for requirements management, it did not do so for cost and schedule estimation, and cybersecurity. Specifically:

- OPM did not fully adopt best practices for developing program cost and schedule estimates. As a result, its estimates were not reliable.
- OPM adopted one key cybersecurity practice for systems engineering and partially adopted four other practices. For example, although OPM had identified security expectations for the migration phase, the agency had not defined the level of service to be supplied by the shared service provider. Following these practices help ensure that security requirements and needs are addressed throughout the life cycle of the system.

Until the agency fully implements appropriate practices, OPM increases the risk that the program will incur schedule delays, cost overruns, unmet performance targets, and cybersecurity shortfalls.

Contents

Letter		1
	Background	5
	OPM Made Initial Modernization Progress, but Is Now Experiencing Schedule Delays	15
	OPM Partially Implemented Modernization Practices	21
	OPM Partially Adopted Selected Leading IT Management Practices	24
	Conclusions	42
	Recommendations for Executive Action	43
	Agency Comments and Our Evaluation	44
Appendix I	Objectives, Scope, and Methodology	47
Appendix II	Comments from the Office of Personnel Management	53
Appendix III	GAO Contact and Staff Acknowledgments	56
Tables		
	Table 1: Status of the Office of Personnel Management's (OPM) Federal Financial System-Replacement (FFS-R)	16
	Table 2: Summary of the Extent to Which the Office of Personnel Management (OPM) Implemented Selected Sound Modernization Practices for the Federal Financial System-Replacement (FFS-R) Project, as of July 2021	22
	Table 3: Selected Capability Maturity Model Integration for Development Leading Practices and Corresponding Activities for Requirements Development and Management	25
	Table 4: Extent to Which the Office of Personnel Management (OPM) Adopted Selected Leading Practices for Requirements Development and Management	26
	Table 5: Four Characteristics and Best Practices of a Reliable Cost Estimate, According to GAO's <i>Cost Estimating and Assessment Guide</i>	28
	Table 6: Assessment of the Office of Personnel Management's (OPM) Trust Funds Modernization (TFM) Program's	

January 2021 Cost Estimate Compared to Cost Estimating Best Practices	29
Table 7: Assessment of Extent to Which the Office of Personnel Management's (OPM) January 2021 Schedule for the Trust Funds Modernization (TFM) Program Met Best Practices	35
Table 8: Extent to Which the Office of Personnel Management (OPM) Adopted Selected Leading Cybersecurity Practices and Corresponding Activities in Its Federal Financial System-Replacement Project, as of July 2021	39

Figures

Figure 1: Office of Personnel Management (OPM)'s Funding Received and Anticipated for the Trust Funds Modernization Program, Excluding Operations and Maintenance Costs, as of July 2021	8
Figure 2: The Six Phases and Related Descriptions of the Modernization and Migration Management Phases	10
Figure 3: Office of Personnel Management's (OPM) Planned Tailored Modernization and Migration Management (M3) Approach for the Federal Financial System-Replacement Project	12

Abbreviations

ARC	Administrative Resource Center
CFO	Chief Financial Officer
CIO	Chief Information Officer
CMMI	Capability Maturity Model Integration
ESC	Executive Steering Committee
FFS	Trust Funds Federal Financial System
FFS-R	Federal Financial System-Replacement
GSA	General Services Administration
IT	information technology
M3	Modernization and Migration Management
NAPA	National Academy of Public Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPM	Office of Personnel Management
RTM	requirements traceability matrix
TFM	Trust Funds Modernization
Treasury	Department of the Treasury
US-CERT	United States Computer Emergency Readiness Team
WBS	work breakdown structure

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



February 23, 2022

The Honorable Chris Van Hollen
Chair
The Honorable Cindy Hyde-Smith
Ranking Member
Subcommittee on Financial Services and General Government
Committee on Appropriations
United States Senate

The Honorable Mike Quigley
Chairman
The Honorable Steve Womack
Ranking Member
Subcommittee on Financial Services and General Government
Committee on Appropriations
House of Representatives

The U.S. Office of Personnel Management’s (OPM) legacy financial system—the Trust Funds Federal Financial System (FFS)—helps manage more than \$1 trillion in combined assets across the federal government’s retirement, health benefits, and life insurance programs. In addition, the system supports over 8 million active federal employees and retirees.¹ However, according to OPM’s April 2020 report to Congress,² FFS is over 20 years old, consists of unsupported software, and its maintenance requires highly specialized staff. In addition, the report noted the system is currently unable to adequately support many of OPM’s accounting and business processes, and presents challenges to the agency’s ability to easily comply with changing laws and regulations.

To address these issues, OPM established the Trust Funds Modernization (TFM) program in fiscal year 2017. TFM consists of several initiatives aimed at automating and streamlining activities in the

¹Federal trust funds are an accounting mechanism used to link dedicated collections with their expenditures for a specific purpose or program. The designation of a trust fund occurs when a law both dedicates collections to a program and identified the account as a “trust fund.” There are four fund types: (1) non-revolving trust fund, (2) special fund, (3) revolving trust fund, and (4) public enterprise fund.

²U.S. Office of Personnel Management, *Report to Congress: Trust Funds Modernization Program*, (Washington, D.C.: April 1, 2020).

accounting processes; the core initiative to modernize FFS is known as Federal Financial System-Replacement (FFS-R). The TFM program is intended to provide stability while FFS is being replaced, reduce manual efforts and time needed to complete financial management, and streamline business processes, among other things. In 2019, OPM selected the Department of the Treasury's (Treasury) Administrative Resource Center (ARC) to be its shared service provider³ to modernize and replace FFS.⁴

The House report accompanying the Consolidated Appropriations Act, 2020 included a provision for us to examine OPM's effort to modernize and replace FFS.⁵ Our specific objectives were to (1) describe the status of OPM's effort to modernize and replace FFS; (2) evaluate the progress OPM has made in implementing modernization practices for using a shared service provider; and (3) determine to what extent the TFM program has adopted leading information technology (IT) management practices for requirements management, cost and schedule estimation, and cybersecurity.

To address the first objective, we reviewed and analyzed relevant information on the FFS-R project such as OPM's report to Congress,⁶ the TFM program schedule and roadmaps—high level overview of milestones presented in a timeline—, risk registers, and executive steering committee meeting minutes.⁷ In addition, we analyzed documentation

³A shared service provider is a government, or commercial entity under the auspices of a government entity, that provides administrative and operational services and processes—such as financial system hosting and financial reporting—that can be shared by multiple organizations within or among agencies.

⁴With ARC's assistance, OPM intends to migrate FFS to ARC's service platform to standardize its business processes and replace the legacy system. ARC is to continue to provide financial management platform system services to OPM after the migration. According to OPM, the agency selected a particular level of service, and going forward, reserves the right to re-assess the service level agreement with proper notice to ARC.

⁵H. Rpt. No. 116-122 at 78-79 (June 19, 2019) accompanying the Consolidated Appropriations Act, 2020, Pub. L. No. 116-93, Division C, 133 Stat. 2317, 2471 (Dec. 20, 2019).

⁶U.S. Office of Personnel Management, *Report to Congress: Trust Funds Modernization Program*, (Washington, D.C.: April 1, 2020).

⁷While the scope of the objective is focused on the FFS-R project, we reviewed TFM program documentation when warranted. TFM program documentation covers the full modernization effort, including the FFS-R project.

completed for each phase of the FFS-R project, such as the interagency agreements and governance documents. Further, we analyzed OPM's TFM risk register to identify open critical risks.

To address the second objective, we selected two modernization practices—performing a comprehensive risk assessment and completing a tollgate review—from the General Services Administration's (GSA) Modernization and Migration Management (M3) guidance used for modernizing financial systems.⁸ We selected those practices that were intended to decrease risk and achieve successful modernizations. To determine the progress OPM had made, we compared the selected practices from the M3 guidance to the agency's modernization program documentation through the Engagement phase,⁹ such as OPM's report to Congress,¹⁰ milestone reports, and executive steering committee meeting minutes.¹¹

To address the third objective, we assessed TFM and FFS-R's policies and practices for managing requirements, cost and schedule estimation, and cybersecurity. Specifically,

- We selected three leading practices associated with requirements development and management in the Software Engineering Institutes' Capability Maturity Model Integration (CMMI) for Development.¹² We

⁸General Services Administration, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); *M3 Playbook Guidance* (Aug. 3, 2016).

⁹A typical modernization and migration following the M3 guidance has six phases: Assessment, Readiness, Selection, Engagement, and Migration. OPM tailored its M3 approach to combine the Assessment, Readiness, and Selection phases into one phase, and divided both the Engagement and Migration phases into two parts. We discuss this further in the body of the report. During the Engagement phase, the agency is to conduct detailed planning by identifying gaps between the requirements and the solution and finalizing the migration approach.

¹⁰U.S. Office of Personnel Management, *Report to Congress: Trust Funds Modernization Program*, (Washington, D.C.: April 1, 2020).

¹¹While the scope of the objective is focused on the FFS-R project, we reviewed TFM program documentation when warranted. TFM program documentation covers the full modernization effort, including the FFS-R project.

¹²Software Engineering Institute, *Capability Maturity Model® Integration for Development*, Version 1.3 (Pittsburgh, Pa.: November 2010).

then evaluated the FFS-R project's documentation, such as the requirements traceability matrix, against the selected practices.

- We reviewed documentation supporting OPM's cost and schedule estimates for the TFM program, which includes the FFS-R project. Specifically, we evaluated documentation supporting the program's January 2021 cost estimate against the best practices for developing a comprehensive, well-documented, accurate, and credible cost estimate identified in GAO's *Cost Estimating and Assessment Guide*.¹³ In addition, we assessed the TFM program integrated master schedule, dated January 2021, and related supporting documentation against leading practices for developing a comprehensive, well-constructed, credible, and controlled schedule identified in GAO's *Schedule Assessment Guide*.¹⁴
- We selected five practices that represented key elements for addressing cybersecurity requirements and needs in an acquisition from the National Institute of Standards and Technology's (NIST) guidance on systems security engineering.¹⁵ We then evaluated the FFS-R project's documentation, including OPM and ARC's interagency agreements, shared service agreement, and acquisition strategy against the selected NIST guidance.

For each objective, we also corroborated our analysis by interviewing agency officials in OPM's TFM Program Management Office and ARC, as well as OPM's Deputy Chief Information Officer (CIO) and the Senior Advisor in the Office of the CIO. Additional details on our objectives, scope, and methodology are provided in appendix I.

We conducted this audit from March 2020 to February 2022 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

¹³GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, [GAO-20-195G](#) (Washington, D.C.: Mar. 12, 2020).

¹⁴GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules*, [GAO-16-89G](#) (Washington, D.C.: Dec. 22, 2015).

¹⁵NIST, *Systems Security Engineering: Considerations for Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Special Publication 800-160, Volume 1 (Gaithersburg, Md.: Mar. 21, 2018).

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

OPM's mission is to lead and serve the federal government in enterprise human resources management. In carrying out its mission, OPM supports the federal workforce by providing benefits to employees, retirees, their survivors, and families. In doing so, OPM relies on its core financial management system that supports its trust fund accounting, FFS. FFS is an application used to record financial transactions and is currently a part of OPM's Benefits Financial Management System, one of the agency's major IT systems. FFS is also one of the key systems that provides data for reports required by legislation such as the Digital Accountability and Transparency Act of 2014.¹⁶

OPM Initiated Efforts to Modernize Its Mission Critical FFS and Related Systems and Processes

As previously mentioned, FFS is outdated, consists of unsupported software, and requires highly specialized staff resources to maintain. In addition, the system is currently unable to adequately support many of OPM's accounting and business processes, and it presents challenges to the agency's ability to easily comply with changing laws and regulations. Further, OPM has not had a support contract in place to receive updates to FFS since 2002, which has contributed to, among other things, security risks inherent with operating an application that no longer receives updates, unmet mission needs, staffing issues, and increased costs. In the absence of a support contract, OPM stated that it employed staff to support FFS.

In fiscal year 2017, OPM created the TFM program to modernize and replace the FFS and to automate and streamline related systems and manual processes. Specifically, the TFM program consists of five initiatives:

- **FFS-R**—this project is the multi-phased, multi-year core modernization initiative focused on replacing the existing FFS and streamlining investment accounting, transaction processing, and debt collection for the trust funds.
- **Payment Process Automation Initiative**—an initiative focused on automating payment transactions (receipts and deposits).

¹⁶Pub. L. No. 113-101, 128 Stat. 1146 (May 9, 2014) codified at 31 U.S.C. § 6101 note. The act expanded the Federal Funding Accountability and Transparency Act of 2006 to increase accountability and transparency in federal spending.

-
- **Headcount Automation**—intended to automate the collection process of retirement and insurance enrollment data used, in part, to determine the Federal Employees Health Benefit plan rates from federal payroll offices.
 - **Direct Premium Remittance System Assessment**—an initiative to develop a long-term cost strategy to manage the collection of the Federal Employees Health Benefit premiums sent to OPM by annuitants.¹⁷
 - **Digital Transformation Initiative**—an initiative intended to leverage automation to transform manual business processes for payments received (e.g., digital document management and robotic process automation which uses technology to mimic human tasks).

As part of the program, OPM established the TFM Program Management Office and the TFM Executive Steering Committee (ESC). The TFM Program Management Office resides within OPM's Office of the Chief Financial Officer (CFO) and is responsible for managing the implementation of the TFM program's five initiatives.

The TFM ESC is responsible for providing direction and guidance for, and monitoring of, the program. The committee is comprised of various agency officials, including the CFO, CIO, associate directors, and the Office of the Inspector General.

To better understand its needs, in 2017, OPM worked with a federally funded research and development center to conduct an independent analysis of its Trust Funds operations.¹⁸ The center performed market research that compared several federal provider solutions, developed an incremental business capability delivery approach for the modernization, and identified risks specific to the modernization. Based on this research, in March 2019, OPM entered into an agreement with ARC to be the agency's shared service provider for the modernization and migration to

¹⁷As of September 2020, the Direct Premium Remittance System received its service from the National Finance Center. However, according to the TFM Program Manager, OPM is assessing the long-term savings and based on the assessment's recommendation, OPM will decide to continue receiving services from the National Finance Center or move to another provider.

¹⁸Federally funded research and development centers are research institutions owned by the federal government but operated by contractors, including universities, nonprofit organizations, and industrial firms. This particular center, the Center for Enterprise Modernization, is sponsored by Treasury, the Department of Veterans Affairs, and the Social Security Administration, and is operated by the MITRE Corporation.

the new system. Following the modernization, OPM plans for ARC to provide the infrastructure, platform, and software services for the operations and maintenance of the system, while OPM performs the transactional processing.¹⁹

In the April 2020 report to Congress, OPM estimated that the total cost to implement the TFM program would be \$58.5 million, excluding operations and maintenance cost, and that the program would be completed by October 2023.²⁰ The agency later estimated operations and maintenance costs would be \$2.7 million annually, beginning in fiscal year 2023.

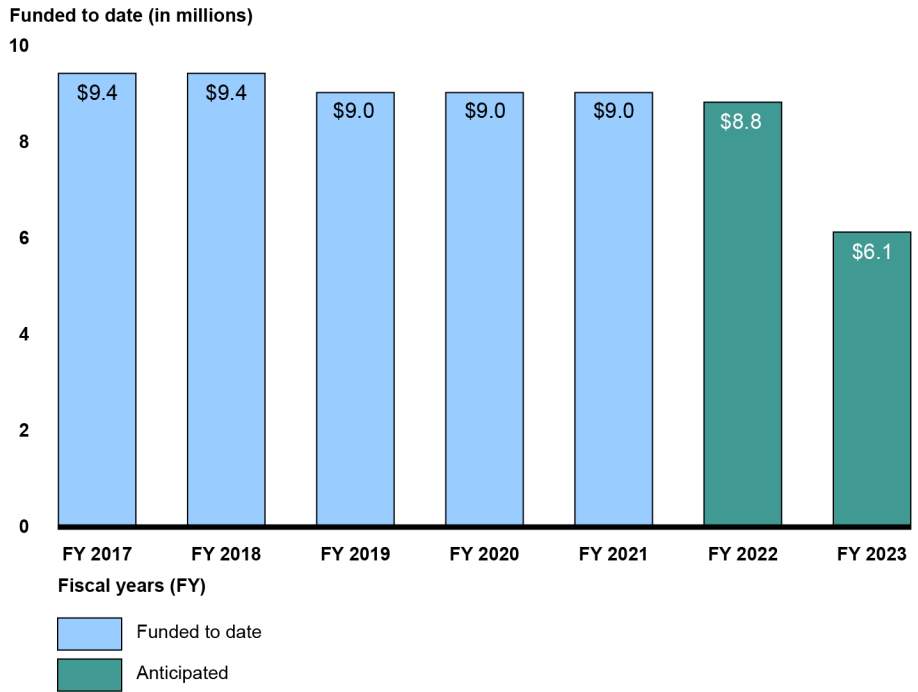
Between fiscal years 2017 and 2021, the agency received a total of approximately \$45.8 million in funding for the program.²¹ The agency requested an additional \$8.8 million for fiscal year 2022 and estimated that the program would need \$6.1 million for the modernization in fiscal year 2023. In total, the estimated cost to develop the TFM program is \$60.7 million, which is about \$2.2 million more than the April 2020 estimate. The agency also planned to request additional funding for operations and maintenance costs in fiscal year 2024, but had not yet identified the amount. Figure 1 provides the funding OPM received and anticipated for the TFM program, excluding operations and maintenance costs, as of July 2021.

¹⁹ARC offers three software-as-a-service levels for its shared service customers, all of which provide the customer with the infrastructure, platform, and software. At the lowest “Platform Service” level, the customer performs all financial management transactional processing. At the next level, known as “Platform Plus Service,” ARC performs some transactional processing. At the “Full Service” level, ARC performs all transactional processing.

²⁰U.S. Office of Personnel Management, *Report to Congress: Trust Funds Modernization Program*, (Washington, D.C.: April 1, 2020).

²¹U.S. Office of Personnel Management, *Report to Congress: Trust Funds Modernization Program*, (Washington, D.C.: April 1, 2020) and *Fiscal Year 2022 Congressional Budget Justification and Annual Performance Plan*, (Washington, D.C.: May 2021) and the *Consolidated Appropriations Act, 2021*, (Pub. L. No. 116-260) H.R. 133- 236 (2020).

Figure 1: Office of Personnel Management (OPM)'s Funding Received and Anticipated for the Trust Funds Modernization Program, Excluding Operations and Maintenance Costs, as of July 2021



Source: GAO analysis of budget information and interviews with the Office of Personnel Management. | GAO-22-104206

OMB and GSA Issued Guidance on Agencies' Use of Shared Services

We have previously reported that the federal government can reduce duplicative efforts and free up resources for mission critical activities by consolidating mission support services—such as financial management—within a smaller number of providers so they can be shared among agencies.²² In May 2016, OMB issued guidance that designated a Shared Services Policy Officer within OMB with the responsibility and authority to develop and implement a government-wide shared services policy,

²²GAO, *Revolving Funds: Additional Pricing and Performance Information for FAA and Treasury Funds Could Enhance Agency Decisions on Shared Services*, [GAO-16-477](#) (Washington, D.C.: May 10, 2016) and *Streamlining Government: OMB and GSA Could Strengthen Their Approach to Implementing a New Shared Services Plan*, [GAO-19-94](#) (Washington, D.C.: Mar. 7, 2019).

among other things.²³ Further, OMB established the Office of Unified Shared Services Management within GSA and tasked the office with bringing stakeholders and agencies together to improve service delivery and performance, and reduce costs to agencies.²⁴

As part of this effort, GSA published the M3 framework, and the related M3 Playbook and guidance. These were based on a collection of leading project management best practices for agencies seeking to modernize their systems and mission support services using a shared service provider.²⁵ GSA developed M3 in coordination with shared services providers, federal agencies, and industry. This work leveraged documents, templates, and leading practice methods used in previous modernizations to support the establishment of a standard set of guidance and documentation.

The framework divides a typical shared services migration into six phases: assessment, readiness, selection, engagement, migration, and operations. For each phase, the framework identifies key steps agencies should take before proceeding, such as completing a risk assessment and mitigation strategies and defining performance and success metrics. In developing its M3 Playbook, GSA provided guidance, tools, and templates intended to reduce the risk and improve the successful outcomes for modernization projects.²⁶

At the end of each phase, the M3 framework recommends that agencies conduct a tollgate—or checkpoint—to assess risk and inform budgeting and funding decisions for the migration. The tollgate review involves

²³OMB, *Improving Administrative Functions Through Shared Services*, OMB M-16-11 (Washington, D.C.: May 4, 2016).

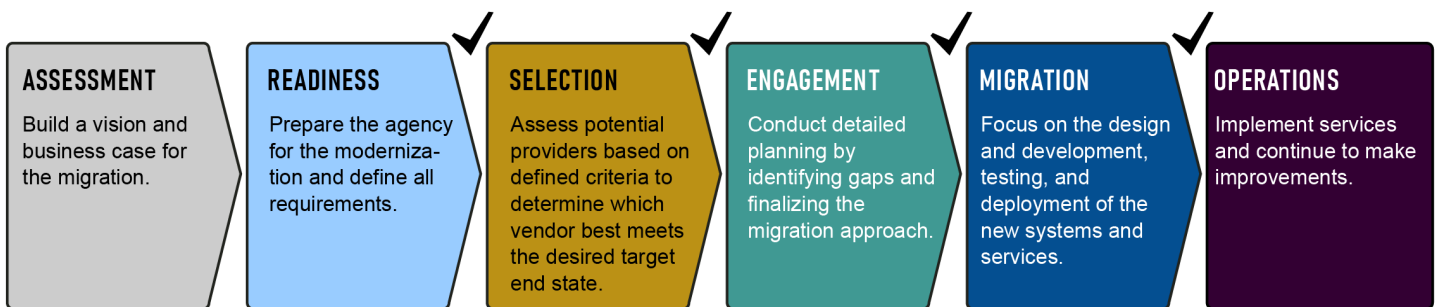
²⁴In 2018, GSA merged the Office of Unified Shared Services Management with the Office of the Executive Councils to form the Office of Shared Solutions and Performance Improvement. This office intended to continue to work with OMB to develop government-wide shared services strategy, policy, and guidance.

²⁵General Services Administration, *M3 Playbook Guidance* (Aug. 3, 2016). In October 2021, GSA's Office of Shared Solutions and Performance Improvement launched an updated M3 Playbook, which includes the Quality Service Management Offices among the stakeholders involved in the modernization process. Although there are some minor differences in activities and outputs, the phases remain the same. In addition, while the updated Playbook has renamed the "tollgate review" to the "progress review," the definition remains the same.

²⁶General Services Administration, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016).

conducting a summary review of the migration with key stakeholders. As part of this, agencies are to complete recommended documentation, including a detailed risk assessment, to obtain approval to continue to the next phase. Figure 2 shows the six phases of the M3 framework and a description of each phase's objective.

Figure 2: The Six Phases and Related Descriptions of the Modernization and Migration Management Phases



✓ Tollgate review

Source: GAO analysis of General Services Administration data. | GAO-22-104206

The M3 Playbook also states that the guidance is not prescriptive; it is guidance for organizations to use to reduce risk and help ensure the successful outcomes of modernizations and migrations. Specifically, the guidance allows agencies to tailor the M3 Playbook activities and resulting outputs to meet their needs. In cases where agencies tailor their M3 processes, GSA recommends that agencies use the M3 Tailoring Guide to determine which of the activities are recommended or optional and document the justification of omitted activities.

In April 2019, OMB issued a memorandum revising its guidance on the shared services approach and GSA's oversight of shared services.²⁷ The memorandum described the process for identifying support functions for sharing and desired outcomes for shared services, and established a governance and accountability model using Quality Service Management Offices. These offices were to offer a marketplace of solutions intended to standardize processes, reduce the technology footprint, improve agency performance in designated mission support areas, and reduce government-wide operating costs. The offices were also to serve as the

²⁷OMB, *Centralized Missions Support Capabilities for the Federal Government*, M-19-16 (Washington, D.C.: Apr. 26, 2019).

lead agencies in the federal government and take responsibility for establishing and managing a marketplace for these solutions.

Further, the guidance designated specific agencies to serve as Quality Service Management Offices for particular service areas and to create an implementation plan for agencies involved in modernization efforts. Notably, in June 2020, OMB designated Treasury as the Quality Service Management Office for the financial management area.

The revised framework also rescinded the May 2016 OMB guidance requiring agencies to use the M3 guidance and removed GSA's required oversight of agencies' progress. Nevertheless, GSA has continued to make the M3 framework available for agencies to use as guidance and best practices for migration and modernization. Most recently, in October 2021, GSA issued an updated version of the M3 playbook and guidance.

OPM Tailored Its M3 Modernization Approach

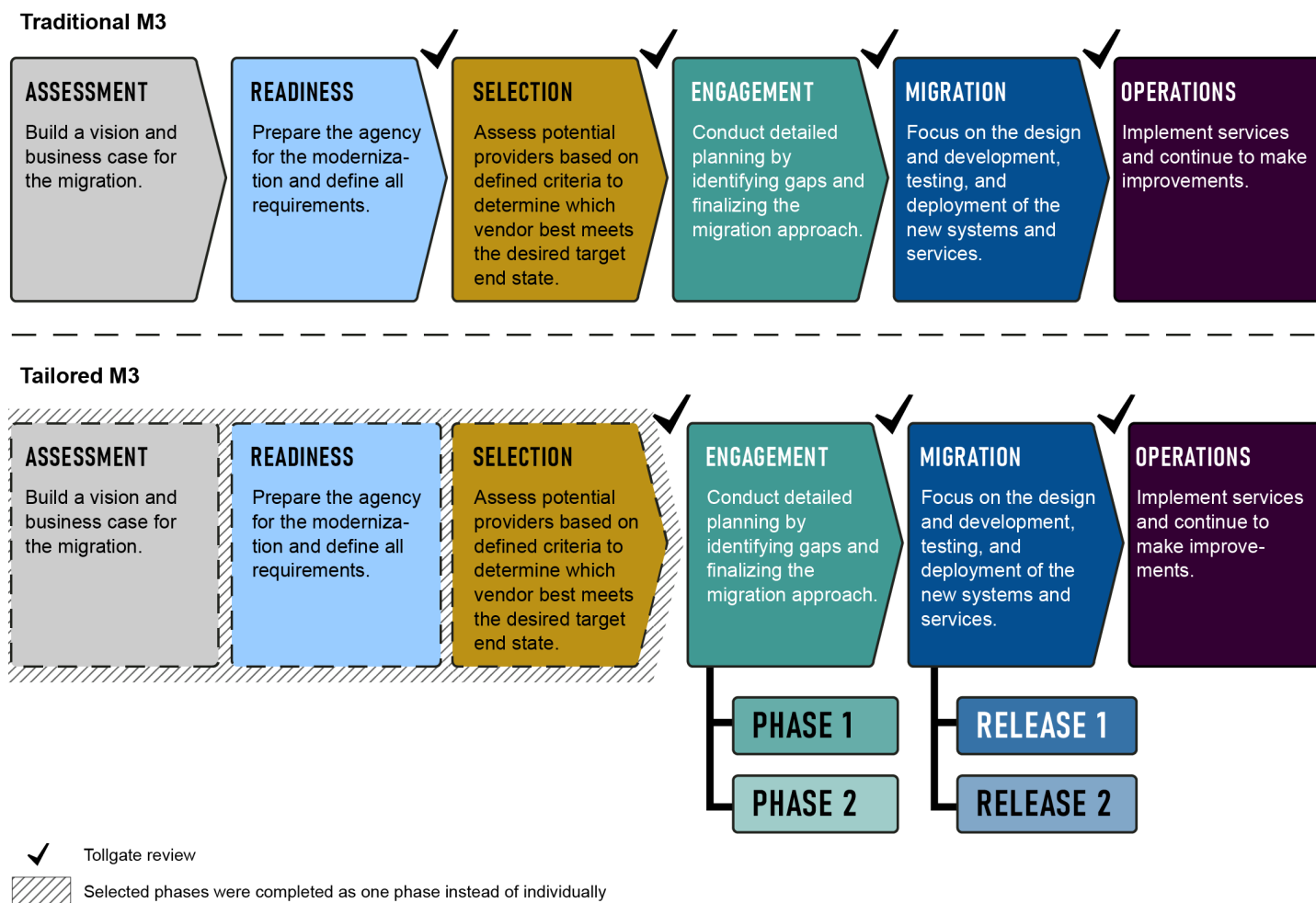
According to OPM, the agency developed a tailored M3 approach for the FFS-R project due to the complexity of the trust funds business processes. Specifically, OPM's tailored approach modified the timing of certain recommended activities and outputs. For example, OPM combined the Assessment, Readiness, and Selection phases into one phase. According to OPM, this phase was completed as part of the aforementioned analysis conducted by the federally funded research and development center.

In addition, according to OPM, the program divided the Engagement and Migration phases into smaller, more manageable blocks.²⁸ Specifically, OPM and ARC divided the Engagement phase into two parts (Engagement Phase 1 and Engagement Phase 2) and conducted tollgate reviews after each phase. In addition, for the Migration phase, OPM developed a multi-release strategy to mitigate resource constraints due to the scale and complexity of the migration to the new system. Further,

²⁸According to our Agile guide, conducting incremental deployments helps project teams to respond quickly to feedback and continuously measure progress, and thus reducing technical and program risk. See GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, [GAO-20-590G](#) (Washington, D.C.: Sept. 28, 2020).

OPM intends to conduct tollgate reviews after each release.²⁹ See figure 3 for a depiction of OPM's tailored approach for the FFS-R project.

Figure 3: Office of Personnel Management's (OPM) Planned Tailored Modernization and Migration Management (M3) Approach for the Federal Financial System-Replacement Project



Source: GAO analysis of Office of Personnel Management and General Services Administration data. | GAO-22-104206

²⁹OPM also delayed the completion of several recommended activities until later in the modernization. For example, instead of completing a decommission plan for the legacy system during the Selection and Engagement phases, OPM will not complete the decommission plan until the Migration phase Release 1. In addition, although the framework recommends that agencies define the service level agreement for operations and maintenance during the Engagement phase, OPM does not plan to do so until the Migration phase.

GAO and Others Have Reported on OPM's IT and Cybersecurity Challenges

We and others have reported on OPM's challenges in implementing and modernizing IT. These challenges included modernizing legacy systems, adequately securing systems, managing an aging technology environment, and addressing a lack of consistent IT leadership and effective IT governance.

- **Modernizing legacy systems.** We have previously reported on OPM's challenges in modernizing other systems.³⁰ For example, in 2019, we reported that OPM did not have complete plans to modernize a particular legacy system consisting of the hardware, software, and service components that supported OPM's IT applications.³¹ As a result, we recommended that the agency identify and document modernization plans including milestones, descriptions for the necessary work, and details for the disposition of the legacy system. The agency agreed with the recommendation and described plans to address it. As of November 2021, the agency had not implemented the recommendation.
- **Adequately securing systems.** We and others have reported on OPM's cybersecurity incidents and persistent IT security concerns. In June 2015, OPM reported an intrusion into its systems that affected the personnel records of about 4.2 million current and former federal employees. In addition, in July 2015, OPM reported that a separate, but related cyber incident had compromised its systems and the files related to background investigations for 21.5 million individuals, which included employee Social Security numbers, residency and education history, among other things. An estimated 22.1 million individuals had some personally identifiable information stolen, with 3.5 million being a victim of both breaches.

In 2017, we reported that since the 2015 data breaches, OPM had made progress in implementing the recommendations of the United

³⁰For example, see: GAO, *Federal Retirement Processing: Applying Information Technology Acquisition Best Practices Could Help OPM Overcome a Long History of Unsuccessful Modernization Efforts*, [GAO-15-277T](#) (Washington, D.C.: Dec. 10, 2014); *Office of Personnel Management: Retirement Modernization Planning and Management Shortcomings Need to Be Addressed*, [GAO-09-529](#) (Washington, D.C.: Apr. 21, 2009); *Office of Personnel Management: Improvements Needed to Ensure Successful Retirement Systems Modernization*, [GAO-08-345](#) (Washington, D.C.: Jan. 31, 2008); and *Office of Personnel Management: Retirement Systems Modernization Program Faces Numerous Challenges*, [GAO-05-237](#) (Washington, D.C.: Feb. 28, 2005).

³¹Due to sensitivity concerns, the report did not provide the names or detailed descriptions of the systems. GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, [GAO-19-471](#) (Washington, D.C.: June 11, 2019).

States Computer Emergency Readiness Team (US-CERT) to bolster OPM's information security practices and controls.³² However, our report also noted that OPM did not consistently update completion dates for outstanding recommendations and did not validate corrective actions taken to address the recommendations.

As a result, we made five additional recommendations to OPM to improve its security over personnel and other sensitive information at the agency. OPM concurred with four of five recommendations and partially concurred with our recommendation to improve the timeliness of validating evidence with addressing the US-CERT recommendations, but did not state the reason for the partial concurrence. As of November 2021, OPM had implemented three of the five public recommendations.

In addition, in October 2017, OPM's Office of the Inspector General reported that the agency's IT environment contained many instances of unsupported software and hardware, where the vendor no longer provided patches, security fixes, or updates for the software.³³ As a result, the report noted that there was increased risk that OPM's IT environment contained known vulnerabilities that would never be patched, and could have been exploited to allow unauthorized access to data.

- **Managing an aging technology environment.** The aforementioned breaches were due, in part, to the age of the agency's systems and infrastructure. At a Congressional hearing on the security breach, OPM's Director stated that the modernization of the agency's IT infrastructure was critical to protecting the agency's data from adversaries.³⁴ The Director also noted that it was not feasible for the agency to implement encryption on old networks, such as those that were breached.

In addition, in March 2021, the National Academy of Public Administration (NAPA) issued a report that described several

³²GAO, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*, [GAO-17-614](#) (Washington, D.C.: Aug. 3, 2017).

³³U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, *Final Audit Report: Federal Information Security Modernization Act Audit Fiscal Year 2017*, Report Number 4A-CI-00-17-020 (Washington, D.C.: Oct. 27, 2017).

³⁴OPM: *Data Breach, Hearing Before the House Committee on Oversight and Government Reform*, 114th Cong. (statement of Director of the Office of Personnel Management Katherine Archuleta).

challenges that OPM faced, including an antiquated technology environment.³⁵ The report stated that certain major events have significantly amplified the impact of the outdated technology environment. Specifically, the 2015 security breach forced OPM and its OCIO to shift focus and divert resources away from its critical IT modernization efforts to address the fallout from the breach. The report further noted that since the agency's OCIO was unable to serve as an efficient internal service provider over the past few years, shadow IT functions have grown across OPM and continued to perpetuate a fragmented approach.³⁶

- **Addressing inconsistent IT leadership and governance.** According to the NAPA report, OPM's OCIO has experienced high turnover in the CIO position together with critical IT leadership vacancies and high number of IT staff vacancies. The report noted that the most recent CIO was the agency's seventh since 2013, and subsequently was appointed as the new Federal CIO in March 2021.³⁷ In addition, the report stated that at one point, OCIO had a vacancy rate of approximately 40 percent.

OPM Made Initial Modernization Progress, but Is Now Experiencing Schedule Delays

Although OPM had completed several phases of the modernization of FFS, the agency began experiencing schedule impacts and increased costs. According to OPM, these issues were due to realizing several risks, including those related to gaps in knowledge and documentation of the legacy processes. Table 1 provides the status of OPM's effort to modernize FFS.

³⁵National Academy of Public Administration for the U.S. Office of Personnel Management, *Elevating Human Capital: Reframing the U.S. Office of Personnel Management's Leadership Imperative*, Academy Project Number: 102253 (Washington D.C.: March 2021). The National Defense Authorization Act for Fiscal Year 2020 directed OPM to work with the National Academy of Public Administration (NAPA) to conduct an independent assessment of the agency's statutory and non-statutory functions, identify associated challenges, and recommend a course of action to address the challenges. National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, Division A, Title XI, subtitle A, 133 Stat 1198, 1602 (Dec. 20, 2019). The report was a congressionally-mandated study of OPM's functions and the associated challenges in executing those functions.

³⁶According to OMB, shadow IT refers to spending on IT that is not fully transparent to the agency CIO and/or IT resources included as a portion of a program that is not primarily of an "IT" purpose but delivers IT capabilities or contains IT resources.

³⁷As of September 2021, OPM has its eighth CIO since 2013.

Table 1: Status of the Office of Personnel Management’s (OPM) Federal Financial System-Replacement (FFS-R)

Phase	Completed or planned completion date
Assessment, Readiness, and Selection	Completed September 2018
Engagement Phase 1	Completed February 2020 ^a
Engagement Phase 2	Completed September 2020 ^a
Migration Release 1	Planned completion by October 2022 ^b (originally estimated to be completed in October 2021)
Migration Release 2	Planned completion by October 2023 ^b (originally estimated to be completed in October 2022)

Legend:

■ = milestones that have been completed

Source: GAO analysis of OPM’s documentation and interviews. | GAO-22-104206

^aFor reporting purposes, we are referring to Engagement Phase 1 and 2’s “go/no-go decision” milestone date as the “completion date.”

^bFor reporting purposes, we are referring to Migration Release 1 and 2’s “go-live” or deployment date as the “completion date.”

OPM Completed Several Phases of the Modernization of Its FFS

As of July 2021, OPM had completed the Assessment, Readiness, Selection, and Engagement (Phase 1 and Phase 2) phases of the FFS modernization, and was making progress on activities in the Migration phase. Specifically, as of July 2021, OPM had completed the following key activities in the different phases:

- As part of the combined Assessment, Readiness, and Selection phases, OPM established the vision statement and high-level business case in the program management plan. The agency also created the project charter, a program management plan, an integrated master schedule, a target state concept of operations, a business needs workbook, and a benefits management plan to define key expected benefits. The agency also defined the program scope outlined in its business needs and conducted a stakeholder analysis to ensure impacted organizations are prepared for the migration. Further, OPM developed the evaluation criteria to assess provider capabilities, created an acquisition strategy, selected ARC to be its shared service provider, and entered into an initial interagency agreement with ARC for the Engagement phases.
- During Engagement Phase 1, OPM compared ARC’s solution to its business needs to understand gaps; completed a high-level gap analysis and preliminary migration strategy; and estimated operations and maintenance costs.

-
- For Engagement Phase 2, OPM gathered detailed functional and technical requirements, and completed detailed gap analysis and a requirements traceability matrix, among other things. In addition, OPM finalized its migration approach, including schedule and cost estimates, and completed an updated life cycle cost estimate, a readiness assessment, a target state concept of operations, and an interagency agreement with ARC for Release 1 of the Migration phase.

As of October 2021, OPM was working on activities in the first release of the Migration phase, which is intended to deploy core financial management and investment management functionality. For instance, OPM intended to validate and verify requirements, develop the configuration and design for ARC's Oracle platform, develop testing environments for OPM and ARC systems, design and test data conversion preparations, and deploy the integrated platform replacing the FFS, among other things. Further, during this phase, OPM also plans to update the interagency agreement with ARC for Migration phase Release 2 and finalize the service level agreements with ARC, among other things.

OPM Experienced Negative Impacts on FFS-R's Cost and Schedule Due to Realized Risks

Despite the progress made on the modernization, OPM began experiencing schedule impacts and increased costs. Specifically, according to OPM's risk register, these negative impacts were due to realizing several risks, including those related to gaps in knowledge and documentation of the legacy processes, system, and associated interface needs; and OCIO resource constraints. In particular, staff from OCIO did not have the requisite system knowledge or documentation to support a thorough understanding of the FFS legacy system or associated interface needs. In addition, according to representatives from OPM's OCIO, staff most knowledgeable about the FFS legacy system were no longer with the TFM Program Management Office. Further, an ARC official stated that OPM lacked adequate documentation on the legacy systems.

To begin to resolve these issues, OPM added work to the project that extended its schedule for the project by 1 year and incurred additional costs. For example, OPM tasked ARC to reverse engineer the system's

interface requirements,³⁸ build an integration layer,³⁹ and develop test plans and scenarios to replicate OPM business cases, increasing the cost of the modernization by \$4 million.

In addition, OPM extended its schedule for Migration Release 1 twice. Specifically, according to OPM's final report for Engagement Phase 2, at ARC's suggestion, OPM first delayed the completion date of Migration Release 1 by 6 months (from October 2021 to April 2022). Then, in January 2021, according to the ARC Program Manager, OPM suggested that ARC extend the timeline an additional 6 months, resulting in an October 2022 completion date⁴⁰ for Release 1. ARC's Program Manager stated that this delay was due to ARC needing to work around OPM's resource constraints. In addition, OPM extended the completion date of Migration Release 2 from October 2022 to October 2023.

OPM and ARC officials acknowledged that planned dates in the schedule have changed, but disagreed that the schedule has incurred any delays. Specifically, officials stated that because the program had not yet baselined the dates provided in the April 2020 report to Congress,⁴¹ the dates were considered notional. However, schedules created after OPM baselined the program's schedule (on June 15, 2020) reflect the 12-month delay. Specifically, the January 2021 schedule shows that the completion date for Migration Release 1 has been extended by 12 months to 24 months from the original baseline schedule (from October 2021 to October 2022).

The extended schedule is also reflected in additional program documentation. Specifically, according to the final report for Engagement

³⁸Reverse engineering is the process of replicating a design by examining and measuring an existing item to develop the technical data necessary to reproduce the item's functionality. GAO, *Defense Logistics Agency: Small Businesses Participate in Reverse Engineering of Spare Parts*, GAO-19-586 (Washington, D.C.: July 31, 2019).

³⁹The integration layer helps the agency's system interact with the provider's system while converting to the new solution, *Office of the Chief Information Officer, Washington State*, accessed June 2, 2021, <https://ocio.wa.gov/enterprise-technology-dictionary/integration-layer>.

⁴⁰For reporting purposes, we are referring to the "go-live" or deployment date for Migration Release 1 and 2 as the "completion date."

⁴¹A baseline schedule includes the originally planned and accepted dates for key deliverables, which serves as a starting point for future comparisons and signifies stakeholder concurrence.

Phase 2, which was completed after the baselined schedule, OPM initially planned for a 12-month deployment for the Migration Release 1 rather than the current 24-month deployment.

Further, according to the program's June 2021 life cycle cost estimate, OPM estimates that the total cost to develop the system will be \$71.9 million, an increase of \$13.4 million over the April 2020 estimate.

OPM Continues to Face Critical Risks Associated with the TFM Program

During its effort to modernize FFS, OPM identified numerous risks. As of May 2021, these included six ongoing critical risks related to the TFM program.⁴²

- **Parallel modernization efforts.** OPM noted that if there were parallel modernization efforts across the agency, then there could be negative impacts to the TFM modernization effort (e.g., resource constraints). OPM initially identified this risk in March 2018. According to agency documentation, OPM initiated several activities to mitigate this risk. For instance, the FFS team planned to participate in meetings for other governance groups, such as the agency-wide Investment Review Board, to understand competing agency efforts and their potential impacts.
- **Lack of dedicated Office of the Chief Information Officer (OCIO) support.** According to OPM, a lack of dedicated support from the OCIO due to resource constraints could result in missed milestones and increased costs. OPM initially identified this risk in March 2018 and, according to its risk register, had initiated several activities to mitigate this risk, including developing approaches to engage with OCIO and developing a resource plan to support the migration. In addition, the TFM program team planned to directly engage the Chief Information Security Officer to develop a security strategy. Further, in April 2021, OPM entered into a contract worth \$2.8 million to assist OCIO with data migration and interface management activities and to help alleviate the resource constraints.
- **Less than expected program funding.** According to OPM, if the program receives less funding than the amount requested, it may have to delay its delivery timeline. OPM initially identified this risk in

⁴²OPM considers a risk as "critical" if the probability of occurrence and the severity of consequence are high or very high. According to OPM's risk management plan, a risk is assigned a high value score if there is between a 66-90 percent chance that the risk will be realized over the life of the project. Similarly, OPM's risk management plan assigns a very high value score if there is a greater than a 90 percent chance that the risk will be realized over the life of the project.

July 2018. The agency attempted to mitigate this risk by developing an incremental delivery strategy for the modernization and holding biweekly briefings with its executives regarding funding issues and challenges. In addition, according to the risk register, in April 2021, OPM met with OMB to discuss program funding.

- **Potential issues with interfacing between OPM and Treasury’s payment system.** In order to process health benefit credit accounts,⁴³ OPM’s systems need to interface with Treasury’s Automated Standard Application for Payments.⁴⁴ According to OPM, if the agency is unable to transition this functionality to Treasury’s system, it will delay the decommissioning of the legacy system and potentially increase the costs and extend the planned schedule of the program. Although OPM initially identified this risk in July 2018, it increased the rating to high risk in May 2021. To mitigate this risk, OPM planned to conduct a high-level assessment of the gaps and incorporate the additional requirements for the solution into the next migration release schedule.
- **Gaps between OPM’s business needs and ARC’s solution.** According to OPM’s risk register, if gaps exist between the agency’s business needs and ARC’s solution, the program may require additional time and resources to complete the modernization, while continuing to depend on legacy systems. OPM initially identified this risk in July 2018. To mitigate this risk, OPM completed a high-level gap analysis in January 2020 (during Engagement Phase 1) and planned to conduct conference room pilots during the Migration phase. According to ARC officials, the conference room pilots are intended to demonstrate custom development and standard system functionality, during the migration phase. In addition, OPM baselined all Release 1 requirements during the Engagement phases; but did not baseline Release 2 requirements. However, it planned to complete the remaining requirements definition documents during the Migration phase. Further, OPM noted possible custom configurations may be needed, which could result in increased costs.

⁴³OPM reviews an experience-rated carrier’s annual accounting statements, which result in processing contingency reserves and letter-of-credit account adjustments. A carrier of an experience-rated health benefit plan receives premiums in the form of an increase to the letter-of-credit account and requests drawdown from the letter-of-credit account for health benefit claims and administrative payments for which the government maintains reserves.

⁴⁴The Automated Standard Application for Payments is a completely electronic payment application for federal agencies to quickly and securely disburse funds to recipient organizations.

OPM Partially Implemented Modernization Practices

- **Insufficient knowledge and documentation regarding Trust Fund business processes.** According to OPM's risk register, if the agency does not have sufficient knowledge and documentation regarding the legacy trust fund business processes, this could lead to the modernized system not meeting OPM's needs. OPM identified this risk in March 2019, and took steps to mitigate this risk by creating a record of as-is documentation and continuing to engage subject matter experts that are no longer with the TFM program office.

As previously mentioned, GSA established a framework of sound modernization practices—called M3—that are intended to help agencies achieve successful shared services migrations. These practices include, among other things, performing risk assessments and conducting tollgate reviews prior to moving to the next phase. Specifically, GSA recommends that agencies:

- **Perform an M3 risk assessment.** GSA recommends that agencies complete a comprehensive M3 risk assessment during the Readiness, Selection, Engagement, and Migration phases. The M3 risk assessment evaluates the program against a standardized set of risk areas, including those related to cybersecurity, schedule, and requirements management to allow agencies to identify areas of potential risk in their modernization efforts.⁴⁵ The M3 risk assessment also provides evaluation criteria and performance metrics to assist agencies in effectively assessing programs' risk.
- **Conduct a tollgate review.** In addition, GSA recommends that agencies conduct a tollgate review—or checkpoint—at the end of the Readiness, Selection, Engagement, and Migration phases to assess the risk of the migration and inform budgeting and funding decisions for the migration. As part of the tollgate reviews, agencies and key stakeholders are to conduct a summary review of key program documentation regarding the program's schedule, risk, life cycle cost estimates, staffing, and procurement management, among other areas. The M3 Playbook also recommends that agencies define exit criteria that must be met before the program progresses to the next phase. For example, according to the M3 Playbook, agencies should have met exit criteria, such as defining a risk and issues management plan by the end of the Readiness phase, and completing a migration

⁴⁵The M3 risk assessment evaluates the program against a set of 12 risk areas, including risks related to data/information, cybersecurity, financial risk, acquisition and procurement, operational risk, reputational risk, schedule, management support, feasibility, technical complexity, requirements management, and organizational and change management.

approach by the end of the Engagement phase in order to move on to the next phase.

Further, OPM’s FFS-R governance documents also require that the agency conduct tollgate reviews, to include meeting exit criteria, at the conclusion of both parts of the Engagement phase. Specifically, OPM’s FFS-R governance plan outlines key artifacts, such as a preliminary migration strategy, cost estimate, and requirements definition documents, required to be completed to meet the exit criteria and pass the Engagement Phase 1 and Phase 2 tollgate reviews.

Table 2 provides a summary of the extent to which OPM implemented the selected sound modernization practices for the FFS-R project, as of July 2021.

Table 2: Summary of the Extent to Which the Office of Personnel Management (OPM) Implemented Selected Sound Modernization Practices for the Federal Financial System-Replacement (FFS-R) Project, as of July 2021

Practice	Readiness and Selection ^a	Engagement Phase 1	Engagement Phase 2
Perform Modernization and Migration Management (M3) risk assessment	Partially implemented	Not applicable ^b	Partially implemented
Conduct tollgate review	Partially implemented	Implemented	Partially implemented

Source: GAO analysis of agency documentation. | GAO-22-104206

Notes:

^aOPM combined these two phases, along with the Assessment phase. M3 does not recommend that agencies implement these practices at the conclusion of the Assessment phase.

^bSince OPM tailored its M3 approach to include two parts of the Engagement phase, this practice does not apply to the first part of the Engagement phase.

OPM partially implemented the practice of performing an M3 risk assessment for each of the applicable phases. Specifically, during the Readiness and Selection phases (which OPM combined), the agency worked with a federally funded research and development center to complete a solution concept assessment that included an assessment of risks. However, this assessment was not comprehensive in that it did not assess all of the risks recommended by the M3 guidance. For example, the assessment did not assess risks related to data migration, stakeholder management, governance, resource availability, funding, schedule, and cybersecurity, among others.

Although OPM performed an M3 risk assessment during Engagement Phase 2, the assessment did not accurately reflect a key risk that the program was facing. Specifically, at the time of this risk assessment, OPM had not defined service level agreements for operations and

maintenance. The M3 guidance states that such agreements should be addressed during the Engagement phase. However, OPM officials intended instead to define service level agreements during the Migration phase, and therefore they did not assess this risk. This omission at the Engagement phase, according to the M3 guidance, is considered a high risk.⁴⁶

Regarding tollgate reviews, OPM fully implemented the practice for Engagement Phase 1. Specifically, prior to moving from Engagement Phase 1 to Phase 2, OPM conducted a tollgate review, including defining and meeting exit criteria.

However, for the Readiness and Selection phase, although OPM held a decision point to determine whether to move forward with the FFS-R project and obtained approval to move to the next phase, it did not define or meet exit criteria. Without defining or meeting exit criteria, management will not have complete information on which to base its decisions regarding the project's future.

Further, for the Engagement Phase 2, although OPM conducted a tollgate review, which included exit criteria, the agency proceeded to the next phase without meeting the exit criteria. For example, despite being a part of OPM's exit criteria for the Engagement Phase 2, OPM had not completed 13 requirements definition documents. Subsequently, in September 2020, even though the program had not fully met exit criteria, the ESC recommended moving the project forward to the Migration phase. According to the ESC meeting minutes, the committee agreed to begin the Migration phase with a short planning period to address any outstanding requirements and close out any outstanding activities. According to the TFM Program Manager, OPM finalized these outstanding activities, such as the incomplete requirements definition documents, over the following months, with the last being completed nine months later, in May 2021. By moving forward without fully meeting important exit criteria, such as completing the requirements documentation, OPM may place the project's scope at risk, as well as increase the risk of cost and schedule impacts.

⁴⁶The M3 risk assessment provides evaluation criteria for each type of risk to assist the agency in assessing the program's risks. In the area of operational risk, a program is rated low risk if it has defined service level agreements for operations and maintenance. A program is rated high risk if it has defined service level agreements, but some critical components appear to be inaccurate or missing.

OPM indicated that it did not fully perform M3 risk assessments or conduct tollgate reviews because it had tailored its M3 approach. Specifically, according to the TFM Program Manager, OPM did not implement these practices for the Readiness and Selection phases because those activities were completed as part of the solution concept assessment conducted by the federally funded research and development center. Nevertheless, the M3 framework provides best practices intended to decrease risk and help ensure successful modernizations. However, by omitting these critical practices, the agency could increase the project's risk of failure, cost increases, and schedule delays.

Without consistently completing and conducting the M3 risk assessment and tollgate reviews prior to the end of each phase and meeting exit criteria, the agency runs the continued risk of further extending timelines, increasing costs, and not completing a successful modernization. Until OPM fully implements these practices at the completion of Migration phase Release 1 and Release 2, the agency will continue to be at risk in its modernization efforts.

OPM Partially Adopted Selected Leading IT Management Practices

Although OPM fully adopted leading practices related to requirements management, it had not fully adopted leading practices related to cost and schedule estimation and cybersecurity. Specifically, OPM had not fully adopted cost and schedule estimation leading practices. As a result, OPM's cost and schedule estimates were unreliable. In addition, OPM had not fully adopted leading cybersecurity practices. For example, the agency partially adopted the practice of identifying and acquiring experts with sufficient systems and cybersecurity expertise to staff the project.

OPM Fully Adopted Leading Practices Related to Requirements Management

According to the Software Engineering Institute's Capability Maturity Model Integration for Development (CMMI-DEV), effective management of IT requirements is critical for ensuring the successful design, development, and delivery of such new systems.⁴⁷ The CMMI-DEV model provides guidance for applying CMMI leading practices that focus on

⁴⁷Software Engineering Institute, *Capability Maturity Model® Integration for Development*, Version 1.3 (Pittsburgh, Pa.: November 2010).

activities for developing quality products and services to meet the needs of customers and end users.⁴⁸

CMMI-DEV identifies three key leading practices that are important for developing and managing requirements: defining, understanding, and tracing requirements. Table 3 summarizes these three key CMMI-DEV leading practices for requirements development and management and their corresponding activities.

Table 3: Selected Capability Maturity Model Integration for Development Leading Practices and Corresponding Activities for Requirements Development and Management

Leading practices	Corresponding activities
Define requirements - The project defined required functionality (functional requirements) and quality attributes (non-functional requirements) through the development of product requirements.	<ul style="list-style-type: none"> • Identify desirable functionality and quality attributes • Develop requirements in technical terms necessary for product and product component design • Develop the requirements for the identified interfaces both internal and external to the product
Understand requirements - The customer and provider reached a shared understanding on the meaning of requirements as a result of requirements analysis and validation.	<ul style="list-style-type: none"> • Analyze operational concepts and scenarios to refine the customer needs, constraints, and interfaces, and to discover new requirements • Explore the adequacy and completeness of requirements by developing product representations (e.g., prototypes, simulations, models, scenarios, and storyboards), and by obtaining feedback about them from relevant stakeholders • Establish objective criteria for the evaluation and acceptance of requirements
Trace requirements - Requirements were traced in a bidirectional manner between individual source requirements to lower level requirements and work products.	<ul style="list-style-type: none"> • Maintain requirements traceability to ensure that the source of lower level requirements is documented • Generate a requirements traceability matrix

Source: GAO analysis of the Software Engineering Institute's Capability Maturity Model Integration for Development, version 1.3 | GAO-22-104206

OPM fully adopted the three selected leading practices for requirements management, as shown in table 4.

⁴⁸The guidance is based on government and industry development best practices generated from the CMMI framework, a basic structure that organized CMMI components and combines them into CMMI constellations and models.

Table 4: Extent to Which the Office of Personnel Management (OPM) Adopted Selected Leading Practices for Requirements Development and Management

Leading practices and corresponding activities	Assessment
<p>Define requirements</p> <ul style="list-style-type: none"> • Identify desirable functionality and quality attributes • Develop requirements in technical terms necessary for product and product component design • Develop the requirements for the identified interfaces both internal and external to the product 	<p>Adopted.</p> <p>OPM identified the desired functionality and quality attributes by holding requirements gathering sessions with stakeholders to identify project requirements for Federal Financial Systems modernization. Specifically, the agency captured project requirements through work sessions with key subject matter experts across OPM and the Administrative Resource Center (ARC), its shared service provider, to document the functional and technical scope required to design and build the solution. According to OPM's Engagement Phase Final Report and Briefing from September 2020, OPM held 20 initial requirements gathering sessions that were conducted over a 6-week span.</p> <p>In addition, OPM developed requirements in technical terms necessary for product and product component design by working with its shared service provider, ARC, to develop activity diagrams for its business processes that described each process and the stakeholders involved.</p> <p>OPM also developed requirements definition documents, which are intended to define requirements or information required for configuring ARC's solution and developing the required interfaces. OPM developed the requirements for the identified interfaces both internal and external to the product. OPM and its shared service provider documented the interfaces on the requirements traceability matrix (RTM).</p>
<p>Understand requirements</p> <ul style="list-style-type: none"> • Establish objective criteria for the evaluation and acceptance of requirements • Analyze operational concepts and scenarios to refine the customer needs, constraints, and interfaces and to discover new requirements • Explore the adequacy and completeness of requirements by developing product representations (e.g., prototypes, simulations, models, scenarios, and storyboards) and by obtaining feedback about them from relevant stakeholders 	<p>Adopted.</p> <p>OPM established objective criteria for the evaluation and acceptance of requirements. OPM's requirements management plan described a checklist comprised of nine criteria used to identify any gaps or mistakes in the requirements prior to a project team review. According to OPM, it held internal meetings and reviews with ARC to ensure that all of the requirements adhered to the criteria as outlined in the requirement gathering approach document. In addition, before performing a fit-gap analysis, OPM and its shared service provider documented feedback and how the feedback was addressed.</p> <p>OPM analyzed operational concepts and scenarios to refine the customer needs, constraints, and interfaces, and to discover new requirements. Specifically, OPM used the RTM to track 15 unique gap analysis documents which are used to document how each requirement would be met, including proposed solutions and concurrence from stakeholders.</p> <p>OPM explored the adequacy and completeness of requirements by developing product representations and by obtaining feedback about them from relevant stakeholders. According to OPM documentation, at the end of Engagement Phase 2, the agency conducted over 50 follow-up sessions to further refine the requirements, including demonstrations, and engaged with stakeholders, including the Office of the Chief Financial Officer and the Office of the Chief Information Officer.</p>

Leading practices and corresponding activities**Assessment**

Trace requirements

- Generate an RTM
- Maintain requirements traceability to ensure that the source of lower level requirements is documented

Adopted.

For the modernization program, OPM and its shared service provider, ARC, developed an RTM. OPM and ARC used the RTM to document and organize data associated with the modernization project requirements. As of September 2020, OPM had documented 519 requirements in the RTM.

OPM maintained requirements traceability to ensure that the source of lower level requirements is documented. For example, the agency documented the source of requirements on the RTM by associating each requirement with a business use case or capability. Additionally, OPM further ensured traceability by including references to gap analysis documents, and the proposed methods of closure for the identified gaps on the RTM, where appropriate.

Source: GAO analysis of OPM's requirements work products based on leading practices from the Software Engineering Institute's Capability Maturity Model Integration for Development, version 1.3. | GAO-22-104206

By adopting leading practices in requirements management, OPM can better ensure that the modernized system will perform as intended, which in turn may limit the risk of scope, schedule, and cost overruns.

OPM's Cost Estimate Was Unreliable

According to GAO's cost guide, 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* (referred to as the cost guide throughout) outlines best practices for developing reliable cost estimates that management can use to make informed decisions.⁴⁹ These practices can be organized into four characteristics—comprehensive, well-documented, accurate, and credible. In addition, for the estimate to be considered reliable, an organization must meet or substantially meet each characteristic. Table 5 summarizes the four characteristics and corresponding best practices of a reliable cost estimate identified in the cost guide.

⁴⁹[GAO-20-195G](#).

Table 5: Four Characteristics and Best Practices of a Reliable Cost Estimate, According to GAO’s *Cost Estimating and Assessment Guide*

Characteristic	Corresponding best practices
Comprehensive	<ul style="list-style-type: none"> The cost estimate includes all life cycle costs. The technical baseline description completely defines the program, reflects the current schedule, and is technically reasonable. The cost estimate is based on a work breakdown structure that is product-oriented, traceable to the statement of work, and at an appropriate level of detail to ensure that cost elements are neither omitted nor double-counted. The cost estimate documents all cost-influencing ground rules and assumptions.
Well-documented	<ul style="list-style-type: none"> The documentation should show the source data used, the reliability of the data, and the estimating methodology used to derive each element’s cost. The documentation describes how the estimate was developed so that a cost analyst unfamiliar with the program could understand what was done and replicate it. The documentation discusses the technical baseline description and the data in the technical baseline are consistent with the cost estimate. The documentation provides evidence that the cost estimate is reviewed and accepted by management.
Accurate	<ul style="list-style-type: none"> The cost estimate is regularly updated to ensure it reflects program changes and actual costs. The cost model was developed by estimating each work breakdown structure element using the best methodology from the data collected. The estimate has been adjusted properly for inflation. The cost estimate contains few, if any, minor mistakes. Variances between planned and actual costs are documented, explained, and reviewed. The estimate is based on a historical record of cost estimating and actual experiences from other comparable programs.
Credible	<ul style="list-style-type: none"> The cost estimate included a sensitivity analysis that identifies a range of possible costs based on varying major assumptions, parameters, and data inputs. A risk and uncertainty analysis was conducted that quantified the imperfectly understood risks and identified the effects of changing key cost driver assumptions and factors. Major cost elements were cross-checked to see if results were similar. An independent cost estimate was conducted by a group outside the acquiring organization to determine whether other estimating methods produce similar results.

Source: GAO analysis of [GAO-20-195G](#). | GAO-22-104206

OPM’s January 2021 TFM program’s cost estimate was unreliable because it did not substantially meet the four characteristics of a reliable cost estimate described in the cost guide.⁵⁰ Specifically, it partially met the comprehensive characteristic, and minimally met the well-documented and accurate characteristics. In addition, the cost estimate did not meet the credible characteristic. The results of our assessment of the characteristics and the best practices are summarized in table 6.

⁵⁰The TFM Program life cycle cost estimate includes total costs for all TFM projects, including the FFS-R project.

Table 6: Assessment of the Office of Personnel Management’s (OPM) Trust Funds Modernization (TFM) Program’s January 2021 Cost Estimate Compared to Cost Estimating Best Practices

Characteristic and corresponding best practices	Assessment	Summary of assessment
<p>Comprehensive</p> <ul style="list-style-type: none"> The cost estimate includes all life cycle costs. The technical baseline description completely defines the program, reflects the current schedule, and is technically reasonable. The cost estimate is based on a work breakdown structure (WBS) that is product-oriented, traceable to the statement of work, and at an appropriate level of detail to ensure that cost elements are neither omitted nor double-counted. The cost estimate documents all cost-influencing ground rules and assumptions. 	<p>❶</p>	<p>Although OPM noted that the cost estimate included the cost for all projects within the TFM program, the agency’s January 2021 cost estimate did not provide enough details to understand what costs were included in the estimate. As a result, we could not validate that the estimate included all of the relevant life cycle costs. In addition, OPM provided multiple documentation sources with cost data; however, it was not possible to determine whether all costs for the Federal Financial System-Replacement (FFS-R) project, as part of the TFM program, were included. Unless the cost estimate accounts for all costs, management will have difficulty successfully planning program resource requirements and making decisions.</p> <p>OPM based its cost estimate on a technical baseline description which substantially defined the program. However, there was not clear traceability between the pieces of the technical baseline documentation and the agency’s process for documenting technical, program, and schedule updates.</p> <p>Although OPM provided a WBS for the FFS-R portion of the TFM program, the WBS only partially aligned with the program management elements and cost estimate. For example, the estimate did not itemize costs, such as equipment costs, or have an associated WBS dictionary that fully defined all work associated with the elements. In addition, OPM’s cost estimating structure contained minimal details, but provided high-level costs for the Engagement phases and both Migration releases. Without a WBS, an organization may have difficulties tracking resources spent, sharing data among programs, and updating the cost estimate with actual costs.</p> <p>Further, although OPM documented assumptions related to the program management, technology development, and implementation, none of the assumptions were explicitly related to the cost estimate or individual cost elements. For management to make informed decisions there should be clear linkages between the technical baseline parameters, assumptions, and cost inputs examined in the sensitivity analysis.</p>

Characteristic and corresponding best practices**Assessment Summary of assessment**

Well-documented

- The documentation should show the source data used, the reliability of the data, and the estimating methodology used to derive each element's cost.
- The documentation describes how the estimate was developed so that a cost analyst unfamiliar with the program could understand what was done and replicate it.
- The documentation discusses the technical baseline description and the data in the technical baseline are consistent with the cost estimate.
- The documentation provides evidence that the cost estimate is reviewed and accepted by management.



OPM asserted that the TFM program lifecycle costs, including the FFS-R project, were documented within the cost estimate, the WBS dictionary, and its Engagement Phase 2 final report. However, OPM did not provide documentation for the life cycle cost estimate that provided methodology, source data, or how developed costs related to the technical baseline. Without good documentation, the program lacks a basis to provide a credible estimate, questions about the approach used to create the estimate may not be answered, and the scope of the analysis will not be defined.

In addition, OPM did not provide documentation supporting the estimate's methodology or development. Consequently, the estimate could not be traced or reproduced by an analyst unfamiliar with the program. Without adequate documentation, an analyst unfamiliar with the program will not be able to replicate the estimate because they will not be provided enough information to make informed decisions.

Although OPM's estimate identified the costs by program development phase, it did not provide technical baseline documentation describing the scope and technical details of the program and its associated costs. Without a technical baseline, the cost estimate will lack specific information regarding technical and program risks.

Further, although OPM briefed the Executive Steering Committee on a cost estimate in January 2021, OPM did not provide evidence that the estimate was reviewed and approved by management. In addition, OPM told us that the Engagement Phase 1 and 2 final reports and the migration timeline, among other documents, were reviewed by management. However, the documents did not contain evidence of approval. If management is not provided sufficient information about how the estimate was constructed—including specific details about the program's estimating ground rules and assumptions, data, cost estimating methodologies, sensitivity, and risk and uncertainty—management will not have confidence that the estimate is complete and high in quality.

Characteristic and corresponding best practices**Assessment Summary of assessment**

Accurate

- The cost estimate is regularly updated to ensure it reflects program changes and actual costs.
- The cost model was developed by estimating each WBS element using the best methodology from the data collected.
- The estimate has been adjusted properly for inflation.
- The cost estimate contains few, if any, minor mistakes.
- Variances between planned and actual costs are documented, explained, and reviewed.
- The estimate is based on a historical record of cost estimating and actual experiences from other comparable programs.



In addition to the January 2021 estimate, OPM provided cost estimates for July 2020 and April 2021 that demonstrated that the estimates had been updated to include changes in cost. For instance, the cost estimate presented by the program at the January 2021 Executive Steering Committee meeting reflected changes such as a \$4 million increase from the original estimate and a revised cost estimate at the end of Engagement Phase 2.

However, the January 2021 estimate provided no information about the estimating methodology or how the estimate was developed for each WBS element. For example, although the estimate was a single point estimate, it did not include information for how the ranges were derived. Without access to a detailed cost model, one cannot be certain that all WBS cost estimate calculations are accurate. Validating that a cost estimate is accurate requires thoroughly understanding and investigating how the cost model was constructed.

In addition, the estimate did not include adjustments for inflation. Agency documentation noted that the use of inflation was not applicable. For example, OPM provided a historical cost model that only reflected the 2020 costs and did not provide a multi-year estimate for the entire life of the program. When adjusting for inflation, if the index is not correct, the resulting estimate could overstate or understate the cost of the program.

We were unable to assess the extent to which the January 2021 cost estimate included errors because the estimate contained only summary-level data for life cycle costs and the price schedule for the interagency agreement performance work statement. Cost models with limited details complicate the ability to determine if all WBS cost estimate calculations are accurate and account for all costs.

OPM provided documentation outlining the agency's intent to manage integrating costs and schedule for the entire TFM program, but did not explain how variances between the planned and actual costs estimates were developed and tracked. Without a documented comparison between the prior estimate and actual costs for the same period of time, the cost estimators cannot determine how well they are estimating the impacts of program changes over time.

OPM did not provide evidence of historical cost data from similar programs or whether the cost data was validated to provide reliable and valid data to manage the program. Specifically, according to OPM's TFM Program Management Plan, the program planned to use earned value management data to monitor costs, among other things. However, OPM did not provide the earned value management data and, therefore, we could not confirm its use for monitoring costs for the TFM program. A lack of historical data will leave the cost estimator without insight into actual costs of similar programs, including cost growth since the original estimate.

Characteristic and corresponding best practices

Assessment Summary of assessment

<p>Credible</p> <ul style="list-style-type: none"> • The cost estimate included a sensitivity analysis that identifies a range of possible costs based on varying major assumptions, parameters, and data inputs. • A risk and uncertainty analysis was conducted that quantified the imperfectly understood risks and identified the effects of changing key cost driver assumptions and factors. • Major cost elements were cross-checked to see if results were similar. • An independent cost estimate was conducted by a group outside the acquiring organization to determine whether other estimating methods produce similar results. 	<p>○</p> <p>OPM did not perform a sensitivity analysis, which includes varying individual assumptions or factors to understand how the cost estimate would be impacted. Failing to conduct a sensitivity analysis increases the chance that decisions will be made without a clear understanding of these impacts on costs.</p> <p>OPM did not conduct a risk and uncertainty analysis. OPM officials noted that conducting those analyses were not applicable because the TFM cost estimate is reviewed monthly and reflects cost drivers. However, OPM provided documentation that identified risks that may have an impact to the Migration phase costs and are assessed qualitatively as low, medium, and high. Without a risk and uncertainty analysis, the program estimate will not reflect the degree of uncertainty, and a level of confidence cannot be given about the estimate.</p> <p>In addition, OPM did not perform cross-checks to ensure that alternative estimating methodologies produce similar results because the independent analysis conducted by a contractor served as the cross check to validate vendor provided costs. However, the contractor’s analysis was not independently validated and used outdated cost data. Unless an estimate employs cross-checks, the estimate will have less credibility because stakeholders will have no assurance that alternative estimating methodologies produced similar results.</p> <p>OPM provided a historical cost estimate based on market research conducted by a contractor as its independent cost estimate. However, the estimate was at a summary level, almost 3 years old, and limited to a single table that provides no context. A program estimate that has not been reconciled with an independent cost estimate has an increased risk of proceeding underfunded because an independent cost estimate provides an objective and unbiased assessment of whether the program estimate can be achieved.</p>
---	---

Legend:

- = Met: The program office provided complete evidence that satisfies the entire criterion.
- = Substantially Met: The program office provided evidence that satisfies a large portion of the criterion.
- ⦿ = Partially Met: The program office provided evidence that satisfies about half the criterion.
- ⦿ = Minimally Met: The program office provided evidence that satisfies a small portion of the criterion.
- = Not Met: The program office provided no evidence that satisfied any of the criterion.

Source: GAO analysis of OPM’s data and [GAO-20-195G](#). |GAO-22-104206

According to the TFM Program Manager, OPM did not ask ARC about the detailed costs it used to create the interagency agreement’s summary cost estimate because ARC agreed to complete the work outlined in the interagency agreement’s performance work statement at the stated cost. Nevertheless, while ARC is responsible for the estimation of FFS-R’s cost, OPM, as the program management entity, should have full insight into and be ultimately accountable for the TFM program’s life cycle cost estimate (including for FFS-R).

In addition, the official stated that our cost estimating best practices were not applicable to the program because OPM is not building a new system, but rather the agency is migrating to a shared service platform. However,

the best practices provided in the cost guide can be used for any acquisition, program, or project activity, such as modernization, not just when an organization is developing a new system. Adhering to the cost estimate best practices identified in our cost guide could help OPM effectively plan, manage, and oversee its modernization efforts. Further, the interagency agreement between OPM and ARC states that the agencies will use our cost guide, as well as other IT laws and industry standards, to ensure a successful outcome.

By implementing a cost estimate that does not reflect the four characteristics of a high-quality, reliable estimate, OPM is making budget decisions based on potentially inaccurate data. As such, the program risks being unable to effectively estimate future funding needs for the TFM program and using unreliable data to make budgetary decisions. As a result, OPM faces an increased risk of cost overruns and unmet performance targets.

OPM's Schedule Was Unreliable

The success of a project depends, in part, on having an integrated and reliable master schedule that defines when and how long work will occur, and how each activity is related to the others. A project's schedule provides not only a road map for systematic project execution, but also the means by which to gauge progress, identify and resolve potential problems, and promote accountability at all levels of the project. GAO's Schedule Assessment Guide identifies best practices for developing and maintaining reliable project schedules. The best practices are grouped into four characteristics of a reliable schedule: comprehensive, well-constructed, credible, and controlled.⁵¹

- **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

⁵¹[GAO-16-89G](#).


represents a true model of the activities that drive the program's earliest completion date and total float⁵² 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 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. Updates to the schedule are accompanied by a schedule narrative that describes salient changes to the network. It is compared to a designated baseline schedule to measure, monitor, and report the program's progress. The baseline schedule is accompanied by a basis 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.

Although OPM's TFM program schedule substantially met the comprehensive characteristic, the schedule partially met the other three characteristics of a reliable schedule. As a result, the schedule was unreliable. Table 7 summarizes our assessment of OPM's January 2021 TFM program schedule.

⁵²Total 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.

Table 7: Assessment of Extent to Which the Office of Personnel Management’s (OPM) January 2021 Schedule for the Trust Funds Modernization (TFM) Program Met Best Practices

Schedule characteristic	Assessment	Summary of assessment
<p>Comprehensive</p> <ul style="list-style-type: none"> • 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. • Establishes the duration of all activities in the same time unit (preferably days) and has specific start and end dates. • 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. 		<p>OPM’s schedule for the TFM program captured all activities, as identified in the work breakdown structure that needed to be accomplished through Migration Release 1. The schedule also contained clear start and finish milestones and the activities mapped to the latest TFM work breakdown structure.</p> <p>OPM’s schedule established durations and allowed for discrete progress measurement for all activities. However, the schedule contained activities with long durations that needed attention. For example, the schedule included activities that had planned start dates in the distant future or within a month of the status date that had not been broken down into activities that are smaller and more manageable. Schedules with too long of a duration increase the likelihood of not having enough detail for effective progress measurement and reporting.</p> <p>OPM did not assign resources to all activities in its schedule. Specifically, the schedule did not have resources assigned to 524 of 2,237 activities for the TFM program. In addition, the schedule included unrealistic resource assignments. Specifically, 35 of the 48 resources in the schedule were over allocated by 200 percent or more. If the current schedule does not allow insight into current or projected allocation of resources, then the risk of the program’s schedule slipping is significantly increased. Moreover, if the schedule does not fully and accurately reflect the program, it will not be an appropriate basis for analyzing or measuring technical work accomplished and may result in unreliable completion dates, time extension requests, and delays.</p>

Schedule characteristic	Assessment	Summary of assessment
<p>Well-constructed</p> <ul style="list-style-type: none"> 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. 	<p>●</p>	<p>OPM’s schedule for the TFM program included summary activities with logic links, and a number of constraints, lags, and leads.^a In addition, there were issues related to the sequencing of activities. For example, 124 (or 4.4 percent) of the project’s remaining activities were not logically sequenced with links to other activities or milestones. In addition, the schedule contained 508 date constraints, which prevented activities from starting or finishing early.</p> <p>OPM identified a critical path for the TFM program schedule. However, the critical path did not describe activities in the schedule that were truly driving the key delivery date for the program. In addition, the schedule included constraints, deadlines, lags, and leads that appeared to be creating artificial critical activities. Without a valid critical path, management may have difficulty identifying and focusing on activities that will detrimentally affect the key project milestones and deliverables if they slip.</p> <p>OPM’s total float values in the schedule were not reasonable. Specifically, there was too much flexibility in the schedule, and activities were able to slip weeks, months, and even years before delaying key milestones. For example, the average total float in the schedule was 709 days, and the median was 819 days. That is, 49.9 percent of activities can slip approximately 819 days, or 3.1 work years, before delaying key milestones. Realistic float values allow managers to see the impact of a delayed activity on future work. Without realistic estimates of float, it can be difficult to know the amount of time one event can slip without impacting the project finish date and incorrect float estimates will result in an invalid critical path.</p>
<p>Credible</p> <ul style="list-style-type: none"> 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. 	<p>●</p>	<p>Although OPM’s schedule responded appropriately when significant delays were introduced into planned activities, it did not exhibit horizontal traceability for all of the reviewed tasks due to constraints and anomalies in the schedule. OPM stated that it used custom filters to show that the schedule can be traced horizontally but did not provide evidence that demonstrated the use of these filters. In addition, there were also inconsistencies between the dates in the schedule when compared to the dates in the performance work statement. OPM’s schedule exhibited vertical traceability, in part, because the data contained in the master schedule served as both the detailed and summary-level schedules for the program office. However, OPM’s finish dates in the schedule did not match finish dates in the performance work statement.</p> <p>Although OPM stated that it considered risk in developing the schedule, OPM did not conduct a schedule risk analysis. Specifically, OPM did not provide evidence that it conducted a schedule risk analysis to predict a level of confidence in meeting the program’s completion date and the level of necessary schedule contingency. Without a schedule risk analysis, the program may not be able to determine the likelihood of meeting its completion date.</p>

Schedule characteristic	Assessment	Summary of assessment
Controlled	●	<p>OPM's schedule for the TFM program was updated periodically. In addition, the majority of activities and milestones within the schedule had associated baseline start and finish dates. However, there were several date anomalies in the schedule. For example, the schedule included 350 activities that remained incomplete with planned start dates in the past and no recorded actual start dates. In addition, the schedule included 359 activities that remained incomplete with finish dates in the past and no recorded actual finish dates. If unfinished work remains in the past, the schedule no longer represents a realistic plan to complete the program, and team members will lose confidence in the schedule. In addition, OPM's January 2021 integrated master schedule did not include a schedule narrative, which provides a log of changes and its effect on the schedule. We reviewed other OPM documentation that included aspects of a schedule narrative, such as status of key milestone dates and deliverables. However, the other documentation did not include necessary elements, such as changes in logic, date constraints, and the effects of these changes on the schedule, which should be updated as the program progresses.</p> <p>OPM created a TFM baseline schedule, and the majority of activities and milestones in the schedule had associated baseline dates. However, the schedule documentation did not include information relating to some project elements, such as the assumptions the project team made when creating the baseline schedule. A corresponding basis document is important because it explains assumptions used in developing the schedule and is essential for validating and defending a baseline schedule.</p>

Legend:

- = Met: The program office provided complete evidence that satisfies the entire criterion.
- = Substantially Met: The program office provided evidence that satisfies a large portion of the criterion.
- = Partially Met: The program office provided evidence that satisfies about half the criterion.
- = Minimally Met: The program office provided evidence that satisfies a small portion of the criterion.
- = Not Met: The program office provided no evidence that satisfied any of the criterion.

Source: GAO analysis of information for OPM's TFM Program and [GAO-16-89G](#). | [GAO-22-104206](#)

^aA lag in the schedule denotes the passage of time between two activities. Lags simply delay the successor activity—no effort or resources are associated with this passage of time. A negative lag, known as a lead, is used to accelerate a successor activity. Leads imply the unusual measurement of negative time and exact foresight about future events. According to our schedule guide, lags and leads should be used judiciously.

According to the TFM Program Manager, the agency experienced challenges with the program's schedule because of vendor and software issues, including gaps in skill and knowledge. Specifically, the program and the vendor used different versions of the same scheduling software, which corrupted the schedule files. As a result, the program had to recreate its schedule at least twice. The official also stated that OPM's new vendor addressed the software challenge by leveraging an older version of the scheduling software that was compatible with the agency's version and now both vendor and agency are using the same software

version. According to that official, the new vendor is also working to resolve the shortcomings indicated in our initial schedule assessment.

By implementing a program schedule that does not fully and accurately reflect the four characteristics of a high quality, reliable estimate, OPM faces an increased risk of uncertainty for analyzing or measuring technical work accomplished and may result in unreliable completion dates, time extension requests, and delays in the TFM program. Such uncertainty may result in the program being unable to determine the likelihood of meeting its originally estimated completion date resulting in increased project costs. In addition, employing an unreliable schedule may cause management to make uninformed decisions related to possible sequences of activities and the flexibility of the schedule according to available resources, among other things.

OPM Did Not Fully Adopt Selected Leading Practices Related to Cybersecurity

NIST's guidance on systems security engineering establishes leading practices for agencies to follow in developing new systems or updating legacy systems.⁵³ The guidance is intended to address security issues from a perspective of stakeholder requirements and protection needs and to use established processes to ensure that such requirements and needs are addressed with the appropriate rigor across the life cycle of the system. The guidelines address the following cybersecurity leading practices: (1) define security aspects for the program; (2) include security requirements as part of system requirements; (3) select a supplier that meets the security criteria; (4) develop an agreement of security needs with the supplier; and (5) identify, acquire, and maintain a pool of skilled systems and cybersecurity personnel. These practices also have numerous corresponding activities.

For the five selected leading cybersecurity practices, OPM fully adopted one cybersecurity practice and partially adopted four. Table 8 provides a summary of the selected leading practices and our assessment of the extent to which OPM adopted them.

⁵³NIST, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Special Publication 800-160, Volume 1 (Gaithersburg, Md.: Mar. 21, 2018).

Table 8: Extent to Which the Office of Personnel Management (OPM) Adopted Selected Leading Cybersecurity Practices and Corresponding Activities in Its Federal Financial System-Replacement Project, as of July 2021

Leading practice and corresponding activities	Assessment
Define security aspects for conducting the acquisition	●
<ul style="list-style-type: none"> The acquisition strategy should define security aspects, such as how the security objectives will be conducted (e.g., steps intended to ensure assets are secured), the protection needs, and security concerns. 	
Include security requirements as part of system requirements	●
<ul style="list-style-type: none"> The security requirements should be integrated with and provided as part of the stakeholder requirements or system requirements. 	
Select one or more suppliers that meet the security criteria	●
<ul style="list-style-type: none"> Subject matters experts should be involved in the selection process. 	
Develop an agreement that includes security requirements and the level of service that will be supplied	●
<ul style="list-style-type: none"> The agreement with the supplier should satisfy the security requirements and the level of services, including the cybersecurity that will be supplied. 	
Identify, acquire, and maintain skilled systems and cybersecurity personnel to staff ongoing projects	●
<ul style="list-style-type: none"> The organization should identify personnel with security relevant expertise involved in the modernization project. The organization should maintain and manage a pool of skilled cybersecurity and systems engineering personnel. 	

Legend:

- = Fully adopted: OPM provided complete evidence that addressed the entire practice;
- = Partially adopted: OPM provided evidence that addressed one or more of the practices, but not all of the practices;
- = Not adopted: OPM did not provide evidence that addressed the practice.

Source: GAO analysis of OPM's data. | GAO-22-104206

Define security aspects for conducting the acquisition. OPM partially adopted this leading practice. Specifically, in its acquisition strategy, the agency included information on OPM's vision for its future financial system and a high-level roadmap for fiscal years 2017 through 2020 outlining specific actions, such as the development of the solution or services acquisition strategy, engaging stakeholders, and acquiring solutions and services, among other things. However, the agency's high-level acquisition strategy lacked key security details, such as how OPM would manage program risks, the protection needs, and security concerns at the program or project level.

According to OPM's TFM Program Manager, OPM did not include this information in its acquisition strategy because it included standard security language in the interagency agreements with ARC. However, the intent of the practice is to plan for security considerations in the acquisition strategy prior to selecting a provider. Further, although the agreements included security aspects, such as concerns and protection

needs, the agreements did not contain information related to how the security objectives would be conducted.⁵⁴ For example, the interagency agreement for the Migration phase included a security objective to perform a security impact analysis and prepare inputs for a security review, but it did not specify how the security impact analysis and reviews would be conducted.

Include security requirements as part of system requirements. OPM fully adopted this leading practice. Specifically, the agency developed a requirements gathering approach for eliciting, collecting, and developing security requirements as part of developing system requirements for the TFM program, including the FFS-R project. In addition, OPM collected and documented 519 system requirements, including 28 security requirements, using an RTM.⁵⁵ Of the 28 security requirements, OPM and ARC determined that ARC's solution would meet six. OPM and ARC were in the process of analyzing the remaining 22 requirements and intended to address them in Release 2 of the Migration phase.

Select one or more suppliers that meet the security criteria. OPM partially adopted this leading practice. As previously mentioned, OPM had an independent assessment conducted of the TFM program and the assessment included compliance with security. However, security-related experts were not involved with OPM's selection of ARC as the shared service provider. According to OPM officials, the agency intended for the OCIO to be involved as the security experts with the authority to select ARC as the shared service provider. Specifically, the CIO and Deputy CIO are voting members of the ESC, the oversight body that approved the selection of ARC as the provider. However, the September 2018 TFM ESC meeting minutes that document the decision to approve ARC as the selected provider show that the CIO and Deputy CIO were not in attendance and did not vote on the decision.⁵⁶

⁵⁴According to ARC, details on how ARC would conduct security objectives are intended to be addressed in the agreements completed during the Operations phase.

⁵⁵The RTM tracks the requirements from creation through design, development, and testing.

⁵⁶OPM's TFM Executive Steering Committee is comprised of voting members which include the CIO and Deputy CIO and non-voting members. The ESC votes to confirm approvals made for cases such as vendor selection. At the September 2018 TFM ESC meeting, a quorum of attendees was present and voted, but the CIO and Deputy CIO were not a part of that meeting.

Develop an agreement that includes security requirements and level of service that will be supplied. OPM partially adopted this leading practice. Specifically, in March 2019, OPM developed an agreement with Treasury for ARC to be OPM's shared service provider. The agreement identified the scope of work that ARC was to perform for Engagement Phase 1 and Engagement Phase 2. For example, in the interagency agreement's performance work statement, during Engagement Phase 1, initial requirements were identified for the system. In addition, during Engagement Phase 2, more detailed requirements were gathered⁵⁷ and analyses were conducted to identify gaps between ARC's system and service options and the business and technical needs of OPM. The interagency agreement also included security requirements, such as data integrity, privacy protection, performing and reporting of security analyses, and change management procedures in the performance work statement. Additionally, the agreement contained security-related activities, such as conducting a security impact analysis.

However, although OPM identified security expectations for the Migration phase in the performance work statement, the agency had not defined the level of services, which will be supplied by the shared service provider.⁵⁸ Although OPM and ARC had not made an official decision on the service level, according to OPM officials, the agencies were proceeding with the assumption that ARC will provide the infrastructure, platform, and software-as-a-service while OPM performs and manages the transactional processes. According to ARC, its operations and maintenance service agreements usually address compliance with cybersecurity practices, to include the completion of security assessment and authorization, annual continuous monitoring and testing, and tracking training. Moving forward it will be important for OPM to ensure cyber practices are included in the agency's agreements with ARC.

Identify, acquire, and maintain skills to staff ongoing projects. OPM partially adopted this leading practice. Specifically, to identify personnel

⁵⁷According to OPM's Engagement phase interagency agreement with ARC, during the detailed requirements gathering, key stakeholders and the project team were to gather and document detailed requirements which were to be analyzed to ensure alignment with ARC's system and processes.

⁵⁸A service level agreement define the levels of service and performance that the agency expects the service provider to meet and uses the information to measure its effectiveness. Organizations should define how these agreements are to be structured such that the IT services and customers are covered in a manner that best suits the organization's needs.

with security relevant expertise, OPM developed a TFM resource management plan that defined skills and qualifications necessary for each role and staff position based on the needs of the TFM program and related projects. This plan contained estimated resources, including IT resources, needed for the program from fiscal years 2017 through 2023. However, the plan did not identify personnel resources with relevant security expertise. For example, although the plan identified IT roles such as IT Project Manager, IT Specialists, and IT Senior Project Manager, it did not identify whether these roles should have cybersecurity expertise.

Regarding managing and maintaining a pool of skilled personnel to staff ongoing projects, OPM developed plans to assist the agency with its resource management by creating staffing tables to address its TFM program needs and other related projects. Despite this, OPM continued to experience resource constraints associated with vacant positions. According to an OPM OCIO official, the vacancies could affect future phases of the TFM program and its related projects. Further, as previously mentioned, OPM identified the lack of OCIO resources as a critical risk to the program and its ongoing projects.

Until the agency establishes an agreement that outlines how the program's security objectives will be conducted and the level of service that will be provided (including cybersecurity), and identifies and acquires sufficient IT and cybersecurity staff to adequately staff the TFM program (including the FFS-R project), the program will be at risk for expending resources on a project that may not meet the security needs of the agency. It also increases the likelihood that adequate cybersecurity will not be built into the new system, resulting in a potentially insecure system.

Conclusions

Trillions of dollars in retirement, health benefits, and life insurance programs support millions of federal employees and retirees that are dependent, in part, on OPM's successful modernization of its legacy financial system, FFS. Despite some progress, OPM's modernization experienced schedule delays and cost increases due to the agency realizing various risks, including those related to poor documentation and limited staff expertise regarding the legacy processes. At the same time, the agency continues to face other critical risks to the modernization program.

OPM partially implemented the selected modernization practices that can help to minimize risks. Specifically, OPM did not consistently perform the recommended comprehensive risk assessments or conduct tollgate

reviews, to include defining and meeting exit criteria, before proceeding from one modernization phase to the next. Inconsistency in applying these critical practices further increases the risk of extending timelines and, increasing costs.

Although OPM fully adopted selected leading practices for requirements management for the modernization effort, it did not do so for estimating cost, schedule, and for ensuring cybersecurity. Without reliable cost and schedule estimates, OPM's management may be unable to make informed decisions and not be able to minimize risks of additional cost overruns and schedule delays. Finally, although OPM partially adopted cybersecurity practices in its initial stages of the modernization, moving forward it will be critical that OPM implements cybersecurity leading practices, such as establishing agreements that include cybersecurity, and identifying and acquiring cybersecurity personnel for the program. Without doing so, its modernized system could have increased vulnerability exploits.

Recommendations for Executive Action

We are making the following five recommendations to OPM:

The Director of OPM should direct the CFO to ensure that the FFS-R project conducts a comprehensive M3 risk assessment and defines and meets exit criteria for the Migration phase Release 1 and Release 2 tollgates before proceeding to the next phase of the modernization. (Recommendation 1)

The Director of OPM should direct the CFO to ensure that the TFM program develops cost estimates using best practices described in GAO's *Cost Estimating and Assessment Guide*. (Recommendation 2)

The Director of OPM should direct the CFO to ensure that the TFM program updates the TFM schedule using best practices described in GAO's *Schedule Assessment Guide*, in particular, by addressing those schedule characteristics that were not substantially or fully met. (Recommendation 3)

The Director of OPM should direct the CFO to ensure that interagency agreements, including service level agreements, identify how security requirements will be conducted and the level of services, including cybersecurity, that will be provided. (Recommendation 4)

The Director of OPM should direct the CFO to ensure that the OCIO and TFM Program Management Office have identified and acquired sufficient

systems and cybersecurity experts to adequately staff the TFM program, including the FFS-R project. (Recommendation 5)

Agency Comments and Our Evaluation

We provided a draft of this report to GSA, Treasury, and OPM for review and comment. GSA stated that it had no comments on the report. Treasury provided technical comments, which we incorporated in the report as appropriate. OPM provided written comments, which are reproduced in appendix II, and technical comment, which we incorporated as appropriate.

In its comments, OPM concurred with two of our five recommendations, partially concurred with two, and did not concur with one recommendation. Specifically, OPM concurred with our third and fourth recommendations to update the program schedule using best practices and ensure that interagency agreements include specific cybersecurity details. OPM stated that it intends to initiate activities in line with the recommendations.

In addition, OPM partially concurred with our first and second recommendations to conduct comprehensive M3 risk assessments and meet exit criteria and ensure that the program develops cost estimates using best practices. Specifically:

- For the first recommendation, OPM noted that although it has used the M3 framework as a guide, it does not believe that a comprehensive M3 assessment would be a prudent use of resources at this time. The agency stated that, moving forward, it will pay attention to the exit criteria for Release 1. In addition, as it refines the project's implementation plans for Release 2, OPM intends to assess them against the M3 playbook.

As stated previously, conducting comprehensive M3 risk assessments and defining and meeting exit criteria help agencies minimize risk and ensure successful modernizations. While paying attention to exit criteria and assessing plans against best practices are good steps to take, OPM should ensure that they meet defined exit criteria before making the decision to go live with the system. Given the issues the program has experienced and the resulting delays, as OPM completes Release 1 and Release 2 of the Migration phase, it will be critical to perform a comprehensive risk assessment. Such a risk assessment could mitigate further delays and minimize the additional use of resources.

-
- For the second recommendation, OPM stated that while the agency understands that developing reliable cost estimates are crucial, it leveraged a tailored approach to the M3 playbook. OPM also stated that the cost estimates for the program were based upon the assessment of a federally funded research and development center, and included market research and assumptions, among other things. The agency further stated that as cost estimates are developed for the remainder of the modernization effort, the TFM program will consult our *Cost Estimating and Assessment Guide*. While the initial cost estimate may have been based upon another entity's assessment, OPM as the program management entity, should have full insight into and be ultimately accountable for the life cycle cost estimate.

In addition, OPM's interagency agreement with Treasury states that the two agencies will use our cost guide to ensure a successful outcome. Only consulting our guide, and not using it to develop future cost estimates, will leave OPM at risk of additional cost overruns.

Finally, OPM did not concur with the recommendation to ensure that the program has identified and acquired sufficient cybersecurity experts to adequately staff the TFM program. Specifically, OPM stated that the CFO worked with OCIO and the TFM program management office to identify cybersecurity experts to adequately staff the TFM program. OPM further stated that the cybersecurity experts identified by OCIO are responsible for verifying connectivity and ensuring system access standards comply with current cybersecurity standards, among other things.

However, as noted earlier, while OPM developed a resource management plan, the plan did not identify personnel resources with relevant cybersecurity expertise. Although OPM may have since identified cybersecurity experts and assigned responsibilities, without first assessing and identifying the program's needs for cybersecurity expertise, the agency will be unable to know whether they have adequate cybersecurity experts with the appropriate qualifications to meet the program and project needs. Further, OPM did not provide evidence to support their assertion that the program has identified and adequately staffed the program with cybersecurity experts.

In addition, OPM stated that the program initially identified the lack of cybersecurity resources as a potential risk in March 2018 and that this risk was fully mitigated and closed in December 2020. However, our analysis of OPM's May 2021 risk register showed that while the program closed the risk associated with cybersecurity resources, the program combined the monitoring of that risk with another related risk (i.e., OCIO

bandwidth constraints). This related risk was still open and being monitored as of May 2021. OPM did not provide additional documentation to demonstrate that this risk has been closed.

Further, OPM stated that the CIO and Deputy CIO hold regular meetings to discuss program status and security-related activities, and the CIO has assigned a point of contact from OCIO to support the TFM program. While these efforts are promising, TFM's early planning efforts with regards to cybersecurity fell short. As a result, according to program documentation and OCIO officials, the OCIO experienced significant staffing issues which affected phases of the TFM program and its related projects. We have reviewed several program documents that note that the lack of cybersecurity-related personnel was an ongoing risk to the program.

As a result, we believe our recommendation is warranted. Until OPM identifies and acquires the cybersecurity experts needed for this modernization effort, it will be at risk for expending resources on a project that may not meet the security needs of the agency.

We are sending copies of this report to the appropriate congressional committees, the Director of OPM, the Secretary of the Treasury, the Administrator of GSA, and other interested parties. In addition, the report is available at no charge on our website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-6151 or walshk@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 III.



Kevin Walsh
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) describe the status of the Office of Personnel Management's (OPM) effort to modernize and replace its Trust Funds Federal Financial System (FFS); (2) evaluate the progress OPM has made in implementing modernization practices for using a shared service provider; and (3) determine to what extent the Trust Funds Modernization (TFM) program has adopted leading information technology (IT) management practices for requirements management, cost and schedule estimation, and cybersecurity.

To address the first objective, we reviewed relevant information on the FFS-R project¹ documentation, such as OPM's report to Congress,² schedule documentation, risk registers, and executive steering committee meeting documents to describe the status of OPM's modernization effort. Specifically, we determined which modernization and migration phases OPM had completed as of July 2021 and the expected completion dates for the remaining phases. Further, we reviewed the documentation OPM completed for each phase of the FFS modernization effort, including documents such as the interagency agreement,³ integrated master schedule, governance documents, and gap analysis documents, among other things. Additionally, we analyzed OPM's TFM risk register, provided as of May 2021, to identify the open critical risks to the modernization and identify any mitigating strategies.

To assess the reliability of the data in the program's risk register, we interviewed relevant OPM program officials responsible for managing risk, such as the TFM Program Manager. We also compared the data to risk-related documentation, including OPM's risk management plan and tested the data to identify missing or incorrect data in key fields such as the risk identification number and risk score. We determined that the data used were sufficiently reliable for describing the status of OPM's modernization effort.

¹The TFM program consists of five initiatives intended to modernize and replace the FFS and automate and streamline the associated accounting processes. One of the initiatives, FFS-R, is the core modernization initiative within the program. The four other initiatives focused on streamlining related business functions such as accounting and debt collection fund processes.

²U.S. Office of Personnel Management, *Report to Congress: Trust Funds Modernization Program*, (Washington, D.C.: April 1, 2020).

³OPM has entered into an agreement with the Department of the Treasury's Administrative Resource Center (ARC) to modernize and replace FFS.

To address the second objective, we reviewed the General Services Administration's Modernization and Migration Management (M3) guidance for modernizing financial systems.⁴ We then selected two practices that were intended to decrease risk and achieve successful modernizations that use shared service providers. The selected practices were: performing M3 risk assessments and conducting tollgate reviews. We analyzed the progress OPM made in implementing these practices in its efforts to modernize and replace FFS, through the Engagement phase.⁵ To do so, we compared the agency's modernization program documentation, such as OPM's report to Congress, milestone reports, and executive steering committee meeting minutes to the selected modernization practices.

To address the third objective, we used leading practices to assess the TFM program and FFS-R project's policies and practices for managing requirements, cost and schedule estimation, and cybersecurity.

- To determine the extent to which OPM had adopted requirements management best practices, we selected three leading practices associated with requirements management in the Software Engineering Institutes' Capability Maturity Model Integration (CMMI) for Development.⁶ We selected practices that represented foundational practices that are important to developing and managing requirements: defining requirements, understanding requirements, and tracing requirements. We then evaluated the FFS-R project's documentation against the key selected practices and determined whether OPM had adopted, partially adopted, or not adopted those

⁴M3 is a framework designed to help the CFO Act agencies achieve successful outcomes and reduce risk during administrative system and service modernization and migrations. The M3 framework is a six-phased approach, which includes key activities and outcomes for each phase and within each phase there are associated activities detailed in the M3 Playbook.

⁵A typical modernization and migration following the M3 guidance has six phases — Assessment, Readiness, Selection, Engagement, and Migration. OPM tailored their M3 approach to combine the Assessment, Readiness, and Selection phases into one phase and divided both the Engagement and Migration phases into two parts. According to M3 guidance, during the Engagement phase, the agency is to conduct detailed planning by identifying gaps between the requirements and the solution and finalizing the migration approach.

⁶Software Engineering Institute, *Capability Maturity Model® Integration for Development*, Version 1.3 (Pittsburgh, Pa.: November 2010).

selected practices.⁷ In particular, we obtained and analyzed OPM's FFS-R project documentation, such as requirements management plans, activity diagrams, business capabilities, requirements gathering approach, gap analysis documents, requirements traceability matrix, requirements traceability log, Executive Steering Committee artifacts, and requirements definition documents. We then evaluated the FFS-R project's documentation against the key selected practices and determined if OPM had adopted, partially adopted, or not adopted those selected practices.

- To assess the reliability of OPM's requirements data, we reviewed FFS documentation for incomplete or erroneous data. We compared the data to other relevant program documentation on requirements, such as the requirements definition documents, requirements management plan, and documentation on the requirements gathering approach. We also interviewed agency officials about the requirements traceability matrix and the procedures for using it. We determined that the data used were sufficiently reliable for the purpose of evaluating the agency's adoption of selected key practices for managing requirements.
- To determine the extent to which OPM had adopted cost estimation best practices, we reviewed documentation supporting OPM's TFM program cost estimates, including the lifecycle cost estimate from January 2021. Specifically, we determined the extent to which OPM adopted leading practices for the cost estimate for the FFS-R modernization project. To do so, we conducted an analysis of the TFM modernization project cost estimate against the best practices in GAO's *Cost Estimating and Assessment Guide*.⁸ These best practices map to four characteristics of a high-quality, reliable cost estimate. Those characteristics are: comprehensive, well-documented, accurate, and credible. In performing our analysis for the TFM program, we determined the extent to which each characteristic was

⁷"Adopted" means OPM provided complete evidence that it fully adopted the activities of the practice. "Partially adopted" means OPM provided evidence showing that it adopted some but not all of the activities of the practice. "Not adopted" means OPM did not provide evidence showing that it adopted any activities of the practice.

⁸GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, [GAO-20-195G](#) (Washington, D.C.: Mar. 12, 2020).

either not met, minimally met, partially met, substantially met, or fully met.⁹

We shared our preliminary findings with program officials to verify that the information on which we based our findings was complete, accurate, and up-to-date. We then discussed our preliminary assessment results with the program management officials. When warranted, we updated our analyses based on the agency's response and additional documentation provided to us. To assess the reliability of the January 2021 cost estimate data that we used to support findings in this report, we evaluated relevant program documentation, such as cost estimating models, as available, to substantiate evidence obtained from interviews with knowledgeable agency officials. We found the data we used to be sufficiently reliable for the purposes of our report.

- To determine the extent to which OPM had adopted schedule estimation best practices, we reviewed documentation supporting OPM's TFM program schedule estimates including the January 2021 integrated master schedule. Specifically, we determined the extent to which the January 2021 schedule was prepared in accordance with best practices that we had previously identified as fundamental to having a reliable schedule. GAO's Schedule Assessment Guide includes 10 best practices that map to four characteristics of a high-quality, reliable schedule.¹⁰ Those characteristics are: comprehensive, well-constructed, credible, and controlled. We then characterized the extent to which each of the 10 scheduling best practices were met; that is, we rated each characteristic as being either: not met, minimally met, partially met, substantially met, or fully met.¹¹ We also

⁹"Not met" means the program provided no evidence that satisfies any of the best practices criterion. "Minimally" means the program provided evidence that satisfies a small portion of the criterion. "Partially" means the program provided evidence that satisfies about half of the criterion. "Substantially" means the program provided evidence that satisfies a large portion of the criterion. "Fully met" means the program provided evidence that completely satisfies the best practices criterion.

¹⁰GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, [GAO-16-89G](#) (Washington, D.C.: Dec. 22, 2015).

¹¹"Not met" means the program provided no evidence that satisfies any of the best practices criterion. "Minimally" means the program provided evidence that satisfies a small portion of the criterion. "Partially" means the program provided evidence that satisfies about half of the criterion. "Substantially" means the program provided evidence that satisfies a large portion of the criterion. "Fully met" means the program provided evidence that completely satisfies the best practices criterion.

interviewed OPM and contractor officials regarding their scheduling practices.

We shared our preliminary findings with program management officials and discussed our preliminary assessment results with the officials for the programs. Where warranted, we updated our analyses based on the agency response and additional documentation provided to us. To assess the reliability of OPM's schedule, we evaluated documentation supporting the schedule, such as the integrated master schedule. 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.¹² We also interviewed OPM program officials responsible for developing and managing the program schedules 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 schedules.

- Finally, to determine the extent that OPM had adopted best practices for cybersecurity, we reviewed documentation related to OPM's interagency agreements, performance work statements, and procurement process. We identified and selected five best practices that represented key elements for addressing cybersecurity requirements and needs in an acquisition from the National Institute of Standards and Technology's guidance on systems security engineering.¹³ The selected key practices are: defining security aspects for how the acquisition would be conducted, including security requirements as part of system requirements, selecting one or more suppliers that meet the security criteria, developing an agreement with supplier to satisfy the security aspects of acquiring the product or service, and identifying and acquiring skilled systems and cybersecurity personnel to staff ongoing projects. We reviewed the FFS-R project's documentation, including OPM and Treasury ARC's interagency agreements, performance work statement, and acquisition strategy. We also reviewed OPM's staffing tables within its resource management plan to identify the relevant cybersecurity roles and personnel required for the FFS-R project. We then evaluated the

¹²[GAO-16-89G](#).

¹³National Institute of Standards and Technology, *Systems Security Engineering: Considerations for Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. Special Publication 800-160, Volume 1 (Gaithersburg, Md.: Mar. 21, 2018).

documentation against the selected best practices to determine if OPM had adopted, partially adopted, or not adopted those selected practices.¹⁴

To supplement our analysis of the documentation collected from OPM, we also corroborated our analysis by interviewing agency officials, including those in OPM's TFM Program Management Office and ARC that were responsible for OPM's TFM program and FFS-R project, and OPM's Deputy Chief Information Officer and the Senior Advisor in the Office in the Chief Information Officer. In addition, we interviewed an official from the General Services Administration to gain an understanding of the M3 framework used by OPM.

We conducted this audit from March 2020 to February 2022 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.

¹⁴"Adopted" means OPM provided complete evidence that satisfied the entire criterion. "Partially adopted" means OPM provided evidence that satisfied a portion of the criterion. "Not adopted" means OPM provided no evidence that satisfies any portion of the criterion.

Appendix II: Comments from the Office of Personnel Management



Chief Financial
Officer

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

February 2, 2022

Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Walsh,

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, *OPM Needs to Adopt Key Practices in Modernizing Legacy Financial System*, GAO-22-104206, GAO job code number 104206.

Responses to your recommendations are provided below.

Recommendation #1: The Director of OPM should direct the CFO to ensure that the FFS-R project conducts a comprehensive M3 risk assessment and defines and meets exit criteria for the Migration phase Release 1 and Release 2 tollgates before proceeding to the next phase of modernization.

Management Response: Partially Concur

Since the inception of the Trust Funds Modernization (TFM) program and the launch of the Federal Financial System replacement (FFS-R) project, OPM has utilized the M3 framework as a guide for best practices and tools including tailoring it to meet the specific needs of OPM and the FFS modernization effort.

However, OPM does not agree that a comprehensive M3 assessment is a prudent use of resources at this time. Additionally, as previously communicated, there will be specific tollgates conducted between Release 1 (Go/No-Go) and Release 2. There is no subsequent next phase of the modernization planned at this time post-Release 2. Moving forward, OPM will pay particular attention to the exit criteria leading up to Release 1, which is scheduled for October 2022. Also, as OPM refines the implementation plans for Release 2, those plans will be assessed against the M3 playbook.

Recommendation #2: The Director of OPM should direct the CFO to ensure that the TFM program develops cost estimates using the best practices described in GAO's Cost Estimating and Assessment Guide.

Management Response: Partially Concur

www.opm.gov

Recruit, Retain, and Honor a World-Class Workforce to Serve the American People

www.usajobs.gov

**Appendix II: Comments from the Office of
Personnel Management**

OPM understands developing reliable TFM program cost estimates are crucial for realistic program planning, budgeting and management as stated in the GAO Cost Estimating and Assessment Guide.

However, OPM leveraged a tailored approach to the GSA USSM M3 Playbook which provides guidance and best practices to improve the successful outcomes of modernizations and migrations such as the FFS Modernization effort. The FFS Modernization cost estimates were based on inputs from the independent assessment of a Federally Funded Research and Development Center (FFRDC) and included market research, risks, objectives, assumptions, and constraints. For the remainder of the FFS modernization effort, as OPM develops cost estimates, the TFM Program will consult the GAO Estimating and Assessment Guide.

Recommendation #3: The Director of OPM should direct the CFO to ensure that the TFM program updates the TFM schedule using best practices described in the GAO Schedule Assessment Guide to address those schedule characteristics that were not substantially or fully met.

Management Response: Concur

During the remainder of the FFS modernization effort, OPM will update the TFM program integrated schedule and particularly the FFS Modernization schedule. OPM will consult the GAO Schedule Assessment Guide to verify that schedule characteristics that were not substantially or fully met are addressed, as appropriate when updating the schedule.

Recommendation #4: The Director of OPM should direct the CFO to ensure that interagency agreements, including service level agreements, identify how security requirements will be conducted and the level of services, including cybersecurity that will be provided.

Management Response: Concur

The current interagency agreement (IAA) with Treasury ARC covers activities related to the Engagement and Migration Phases of the FFS modernization effort. Requirement elicitation activities for the modernized solution were captured during the Engagement Phase. While the specific security requirements are not explicitly stated in the IAA, the current IAA does include a requirement that ARC must conduct requirements elicitation activities for all requirements, which includes security.

When OPM modifies the current interagency agreement with Treasury ARC for operational support, OPM will clarify the necessary level of services to be provided explicitly include security requirements such as cybersecurity.

Recommendation #5: The Director of OPM should direct the CFO to ensure that the OCIO and TFM program management office have identified and acquired sufficient systems and cybersecurity experts to adequately staff the TFM program, including the FFS-R project.

Management Response: Do Not Concur

**Appendix II: Comments from the Office of
Personnel Management**

The OPM CFO has worked with the OPM OCIO and the TFM program management office to ensure that the necessary support related to systems and cybersecurity experts have been identified to adequately staff the TFM program, including the FFS-R project.

The assigned OPM OCIO cybersecurity experts have been managing and providing guidance on ISA MOU updates. The OPM OCIO cybersecurity experts are responsible for verifying that all the connectivity and system access standards comply with current cybersecurity standards. In addition, they are also responsible for confirming that all the Authority to Operation (ATO) requirements of a Shared Service Provider are being met.

Specifically, the CIO has assigned an OCIO POC to support the TFM program and there is a bi-weekly meeting with the TFM Program Manager and the CIO and Deputy CIO to discuss TFM program status and any technical and/or security related activities.

Additionally, there is a weekly OCIO touchpoint meeting and a bi-weekly TFM touchpoint with the cybersecurity team and the TFM program office to discuss TFM program status and any technical and/or security related activities. In March 2018, the TFM program initially identified a potential risk related to cybersecurity resource availability and outlined mitigation actions to include direct engagement with the CISO and inclusion of the OCIO security resources on various TFM-related project working groups. This risk was fully mitigated and closed in December 2020. All remaining risks associated to OCIO resource availability have been adequately mitigated.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Mr. Mark W. Lambert, Acting Director, Internal Oversight and Compliance, (202) 606-2360, mark.lambert@opm.gov.

Sincerely,

Douglas Glenn
Chief Financial Officer
Office of the Chief Financial Officer

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Kevin Walsh, (202) 512-6151 or walshk@gao.gov

Staff Acknowledgments

In addition to the contacts listed above, the following staff made significant contributions to this report: Jessica Waselkow (assistant director), Melina Asencio (analyst in charge), Chris Businsky, Stephen Duraiswamy, Donna Epler, Rebecca Eyler, Yvette Gutierrez, Anna Irvine, Jason Lee, David Matcham, Ahsan Nasar, Monica Perez-Nelson, Keith Shearer, and Sejal Sheth.

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 our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

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 [Email 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/about/what-gao-does/fraudnet>

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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

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



Please Print on Recycled Paper.