United States Government Accountability Office

Report to the Committee on Homeland Security, House of Representatives

February 2023

DHS FINANCIAL MANAGEMENT

Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues

GAO-23-105194

February 2023

DHS FINANCIAL MANAGEMENT

Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues

GAO Highlights

Highlights of GAO-23-105194, a report to the Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Since DHS's creation in 2003, it has faced significant internal control and financial management systems deficiencies. These issues contributed to GAO designating DHS financial management as high risk. To address its financial management issues, DHS is executing a multiyear plan, to include implementing modern financial management systems at its components, including Coast Guard, FEMA, and ICE.

In this report, GAO (1) describes the oversight, program management, plans, and lessons learned from past and current financial systems modernization efforts; (2) examines the extent to which the Coast Guard is achieving expected capabilities with its newly deployed financial management system; and (3) examines the extent to which Coast Guard has addressed audit findings related to financial reporting and IT system weaknesses.

GAO met with DHS officials, reviewed key documents and plans related to modernization efforts, and assessed Coast Guard corrective action plans to address fiscal year 2021 audit findings.

What GAO Recommends

GAO is making four recommendations, including that the Joint Program Management Office work with Coast Guard, FEMA, and ICE to remediate issues identified by testing; and that Coast Guard follow applicable guidance when developing corrective action plans. DHS concurred with the recommendations and described actions it has taken and will take to address them.

View GAO-23-105194. For more information, contact Paula M. Rascona at (202) 512-9816 or rasconap@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) has defined and implemented a tiered governance structure to provide oversight of its financial systems modernization programs. In 2018, DHS also established the Joint Program Management Office to lead all aspects of the modernization programs, in partnership with DHS components. DHS has both department-level and program-specific plans to modernize financial systems. Financial systems modernization plans at selected DHS components include U.S. Coast Guard, Federal Emergency Management Agency (FEMA), and U.S. Immigration and Customs Enforcement (ICE), among others.

- **Coast Guard** deployed its new financial management system in December 2021 as part of a $510 million modernization program, and declared initial operational capability in June 2022. However, Coast Guard did not achieve expected full operational capability in December 2022. The program office is developing a remediation plan.
- **FEMA and ICE** are in the planning phases of their financial systems modernization efforts. In November 2022, DHS awarded contracts for software licenses and stated that it plans to award contracts for system integration services for these components.

Additionally, DHS established a process and continues to document and consider lessons learned from current and past modernization attempts. These lessons are to be shared with upcoming modernization programs.

Although DHS identified, documented, and tracked metrics to assess Coast Guard's system deployment, DHS found that the system was not achieving expected capabilities. This is because DHS did not address and remediate known issues identified in operational testing. DHS's subsequent operational testing and evaluation of the system found that it was not effective, responsive, or reliable. Therefore, DHS could not proceed to full operational capability of the system. It is now in the process of developing a remediation plan to address outstanding issues.

DHS risks not fully achieving its goal of deploying systems that produce reliable data for management decision-making and financial reporting if it does not remediate serious issues identified by testing. Resolving deficiencies identified by testing before proceeding to the next phase in the acquisition process can help reduce the risk that future system modernization efforts at FEMA and ICE will not meet mission needs or expected capabilities.

GAO also found that corrective action plans Coast Guard developed to address its fiscal year 2021 audit findings did not always contain all of the data attributes recommended in applicable guidance. For example, although DHS guidance emphasizes the importance of root cause analyses in resolving deficiencies, such analyses were often not done. Therefore, Coast Guard is at an increased risk that its corrective actions will not effectively address identified deficiencies.

Contents

Tables

Figures

Abbreviations

ADE	acquisition decision event
CAS	Core Accounting System
CFO	Chief Financial Officer
CISA	Cybersecurity and Infrastructure Security Agency
CWMD	Countering Weapons of Mass Destruction Office
DHS	Department of Homeland Security
DMO	Departmental Management and Operations
DOD	Department of Defense
FEMA	Federal Emergency Management Agency
FFMIA	Federal Financial Management Improvement Act of 1996
FSM	financial systems modernization
FSMS	Financial Systems Modernization Solution
ICE	U.S. Immigration and Customs Enforcement
ICOFR	internal control over financial reporting
J-CONOPS	*Joint Concept of Operations*
J-ORD	*Joint Operational Requirements Document*
JPMO	Joint Program Management Office
KPP	key performance parameter
MAP	mission action plan
NFR	notice of findings and recommendations
O&M	operations and maintenance
OMB	Office of Management and Budget
POA&M	plan of action and milestones
PMP	program management plan
S&T	Science and Technology Directorate
SER	*System Evaluation Report*
SME	subject matter expert
TSA	Transportation Security Administration
USCIS	U.S. Citizenship and Immigration Services

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

February 28, 2023

The Honorable Mark E. Green, MD
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

In our 2021 high-risk update, we reported that much work remains to modernize Department of Homeland Security (DHS) components' financial management systems and business processes to give the department ready access to reliable information for informed decision-making.[1] DHS is executing a multiyear plan to implement modern financial management systems at three of its components, among others: U.S. Coast Guard, the Federal Emergency Management Agency (FEMA), and U.S. Immigration and Customs Enforcement (ICE).[2] These three components constitute a portion of the DHS high-risk designation, and they are the focus of this report.

In fiscal year 2022, Coast Guard transitioned to its new financial management system as part of a $510 million modernization program, and both FEMA and ICE were in the initial stages of procuring financial management software.[3] DHS intends for these modernized systems to help its financial management systems comply substantially with three

[1]GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[2]For fiscal year 2022, FEMA, ICE and Coast Guard were 36 percent, 10 percent, and 17 percent of DHS's total net cost of operations, respectively.

[3]Coast Guard is one of three components that transitioned to the new system under one financial system modernization program, and the life cycle cost estimate includes all three components. In addition, FEMA and ICE are under two separate financial system modernization programs; the life cycle cost estimates for those two programs are not available at this time.

key requirements of the Federal Financial Management Improvement Act of 1996 (FFMIA).[4]

We performed our work under the authority of the Comptroller General to oversee the high-risk area of Strengthening DHS Management Functions, including financial management systems modernization efforts.[5] This report (1) describes DHS's oversight and management of its financial systems modernization (FSM) efforts, modernization plans at selected components, and lessons learned from past and current FSM efforts; (2) examines the extent to which DHS has achieved expected capabilities for Coast Guard's newly deployed financial management system; and (3) examines the extent to which Coast Guard has taken actions to address audit findings related to financial reporting and IT system weaknesses.

To address our first objective, we met with DHS officials to discuss key documents we reviewed that describe the current governance structure and oversight procedures as well as the current financial management systems environment at Coast Guard, FEMA, and ICE. We reviewed DHS's descriptions and plans for the future financial management systems environment at these three components. We also summarized the lessons learned register from current and prior modernization efforts, including the implementation of the new financial management system at Coast Guard.

To address our second objective, we reviewed documentation of the metrics DHS and Coast Guard used to assess the capabilities and the

[4]FFMIA requires 24 federal executive agencies, including DHS, to implement and maintain federal management systems that comply substantially with (1) federal financial management system requirements, (2) applicable federal accounting standards, and (3) the *U.S. Standard General Ledger* at the transaction level. Pub. L. No. 104-208, div. A, § 101(f), title VIII, 110 Stat. 3009, 3009-389 (Sept. 30, 1996), *reprinted in* 31 U.S.C. § 3512 note.

[5]Section 806 of FFMIA defines "financial management systems" as including the financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. Section 806 defines a "financial system" as including an information system, comprising one or more applications, that is used for (1) collecting, processing, maintaining, transmitting, or reporting data about financial events; (2) supporting financial planning or budgeting activities; (3) accumulating and reporting cost information; or (4) supporting the preparation of financial statements. Section 806 defines a "mixed system" as an information system that supports both financial and nonfinancial functions of the federal government or its components. Pub. L. No. 104-208, div. A, § 101(f), title VIII, 110 Stat. 3009, 3009-389 (Sept. 30, 1996), *reprinted in* 31 U.S.C. § 3512 note.

implementation status of the financial management system at Coast Guard called the Financial Systems Modernization Solution (FSMS). We met with DHS officials to gain an understanding of DHS and Coast Guard's process for assessing capabilities by identifying, measuring, and tracking key metrics for implementing FSMS.

To address our third objective, we analyzed corrective action plans that Coast Guard developed to address fiscal year 2021 financial statement auditor–identified findings related to controls over financial reporting and IT systems. We also reviewed findings related to financial management systems not complying substantially with FFMIA requirements. Appendix I provides additional details on our scope and methodology.

We conducted this performance audit from March 2021 to February 2023 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.

Background

DHS High-Risk Financial Management

Since DHS's creation in 2003, significant internal control and financial management system deficiencies have hampered its ability to reasonably assure effective financial and operations management. These deficiencies contributed to our decision to designate DHS's management functions, including financial management, as high risk.[6] In 2010, we identified, and DHS agreed, that achieving 30 specific measurable actions or outcomes would be critical to addressing the challenges within the department's management areas, including eight financial management outcomes. Although DHS has made significant progress in the other management functions, six financial management outcomes are not yet fully addressed. See appendix II for the DHS high-risk financial

[6]GAO's high-risk program started in 1990 and focuses on government operations with greater vulnerabilities to fraud, waste, abuse, and mismanagement, or that are in need of transformation to address economy, efficiency, or effectiveness challenges. Generally coinciding with the start of each new Congress, we have reported on the status of progress addressing high-risk areas and have updated the High Risk List. Overall, this program has served to identify and help resolve serious weaknesses in areas that involve substantial resources and provide critical services to the public.

management actions and outcomes and their status as of November 2022.

Financial Management System Modernization Efforts

DHS has had several initiatives to develop an integrated and comprehensive financial management system, with multiple previous attempts to achieve a department-wide solution.[7] In fiscal year 2018, DHS established a Joint Program Management Office (JPMO) to oversee and manage DHS's current FSM efforts at the component level. There are currently three FSM acquisition programs—FSM-Trio, FSM-FEMA, and FSM-Cube.

Under DHS and JPMO oversight, three DHS components—Countering Weapons of Mass Destruction Office (CWMD), Transportation Security Administration (TSA), and Coast Guard—collectively known as FSM-Trio—transitioned to the new financial management system, FSMS, in three phases:

- CWMD in fiscal year 2018,[8]
- TSA in fiscal year 2021, and
- Coast Guard in fiscal year 2022.

In its fiscal year 2022 agency financial report, DHS stated that it is leveraging the lessons learned from the TSA and Coast Guard implementations to inform future financial management systems modernization efforts, including FEMA and ICE. FEMA's modernization efforts are under its own FSM-FEMA program. ICE and its customer agencies are part of the FSM-Cube program.[9] This report focuses on ICE, a part of the FSM-Cube program, because ICE is an element of the DHS high-risk designation.

DHS approved and initiated its current acquisition programs for financial management system modernization efforts at FEMA and ICE in the

[7]For more information on past DHS financial management system modernization efforts, see app. III.

[8]In 2016, CWMD initially transitioned to a new financial system at its federal shared service provider—the Department of the Interior's Interior Business Center.

[9]The FSM-Cube program includes ICE and its financial management customers—Cybersecurity and Infrastructure Security Agency, Departmental Management and Operations, Science and Technology Directorate, and U.S. Citizenship and Immigration Services.

second quarter of fiscal year 2021. Early DHS estimates currently indicate that FEMA and ICE will transition to their new financial management systems in fiscal years 2025 and 2026, respectively.[10] However, DHS officials stated that those dates are likely to change as the programs go through the planning process.

DHS Audit Requirements

In October 2004, seeking to improve DHS's financial management, Congress and the President enacted the Department of Homeland Security Financial Accountability Act, which, among other things, designated DHS as a Chief Financial Officers (CFO) Act agency.[11] Financial reporting requirements are applicable to all executive agencies, such as the requirement to prepare annual agency-wide audited financial statements.[12] CFO Act agencies must also implement and maintain financial management systems that comply substantially with FFMIA requirements. The DHS Financial Accountability Act also required DHS to obtain an audit opinion on its internal control over financial reporting after fiscal year 2005, making DHS the only CFO Act agency explicitly required by law to do so.

Financial audits are intended to provide independent assessments on the reliability of the financial statements included in the DHS agency financial report. For example, the audits help to provide Congress and the public with transparency and assess how DHS uses its funds. They also help identify and contribute to needed improvements in IT system vulnerabilities and cybersecurity. In addition, audits can identify opportunities for improving DHS's business processes and internal controls.

DHS has received an unmodified (clean) audit opinion on its financial statements for 10 consecutive years—fiscal years 2013 to 2022.[13] However, for fiscal year 2022 DHS's auditors continued to report, for the

[10]ICE and its customer agencies have their own implementation schedules with FSM-Cube implementation for all customer agencies initially estimated for fiscal year 2027.

[11]Department of Homeland Security Financial Accountability Act, Pub. L. No. 108-330, 118 Stat. 1275 (Oct. 16, 2004). CFO Act agencies are those federal executive agencies listed in 31 U.S.C. § 901(b), which currently includes 24 such agencies.

[12]31 U.S.C. § 3515.

[13]An unmodified opinion, sometimes referred to as a clean opinion, is expressed when the auditor concludes that management has presented the financial statements fairly and in accordance with U.S. generally accepted accounting principles.

10th consecutive year, an adverse opinion on internal controls over financial reporting because of material weaknesses in internal controls in the areas of (1) IT controls and information systems and (2) financial reporting.[14]

In addition, for fiscal year 2022, they also reported two new material weaknesses. One of the reported weaknesses related to the controls over the estimation process for insurance liabilities that was elevated from a prior significant deficiency and remained unresolved. The second new material weakness was reported for Coast Guard's newly implemented financial management system's ineffective design of controls over obligations and expenditures. Auditors also continued to report that agency financial management systems did not comply substantially with FFMIA requirements (referred to as FFMIA noncompliance for purposes of this report).

During its financial statement audit, the auditor is to communicate individual audit findings to DHS and its components through notices of findings and recommendations (NFR).[15] After receiving an NFR from auditors, DHS and component management are to develop one or more corrective action plans. The corrective action plans are to outline how the finding will be remediated; establish key milestones, including projected implementation and validation dates; and assign responsibility for completing identified tasks.

[14]A material weakness is a deficiency or combination of deficiencies in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis.

[15]NFRs outline the condition, criteria, cause, effect, and recommendation(s) to correct specific issue(s) that auditors identified in connection with DHS and component financial statement audits.

DHS Established an Oversight Structure, Plans, and a Lessons-Learned Process for Its FSM

Governance Structure and Acquisition Framework

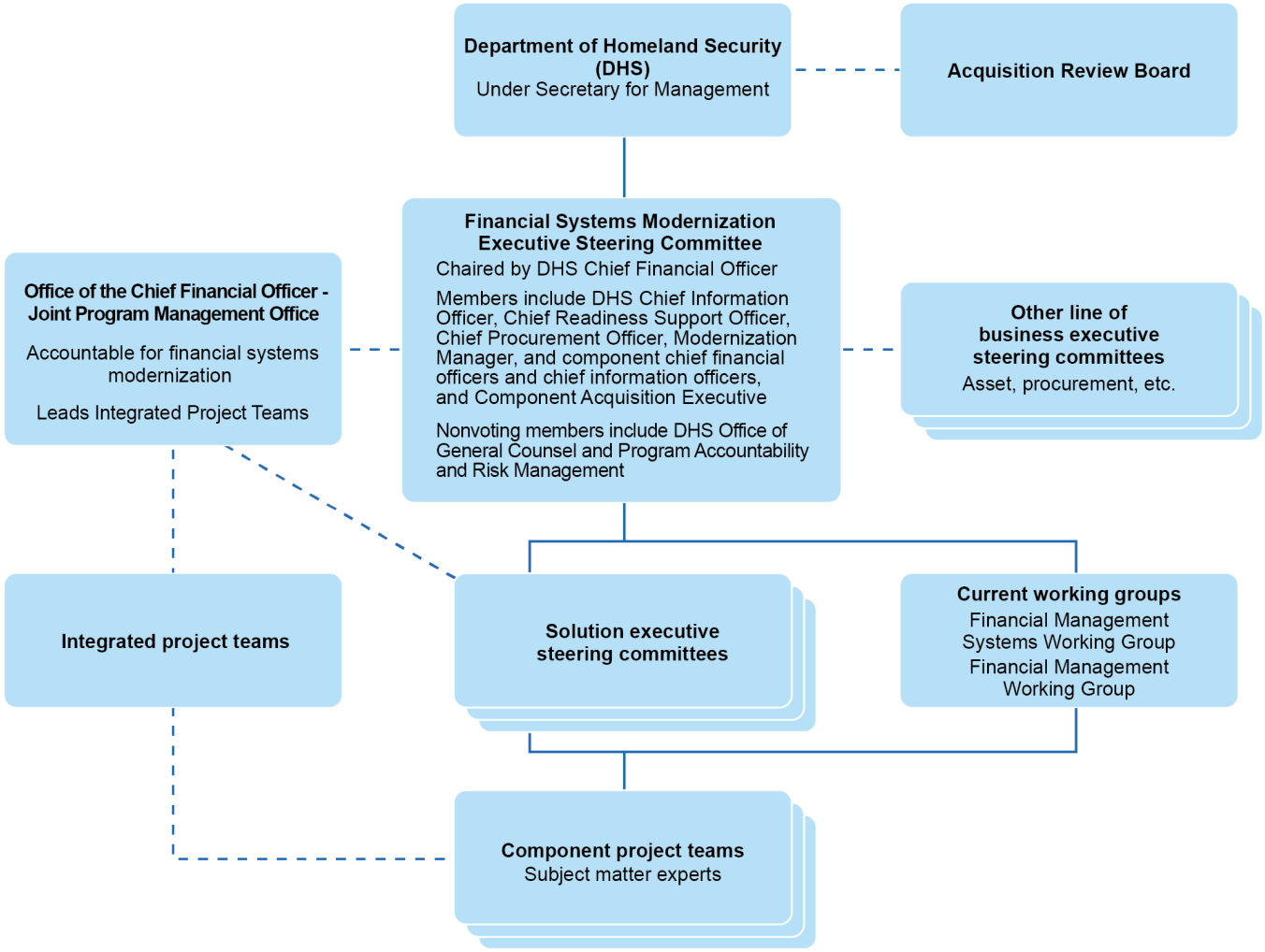
DHS has defined and implemented a tiered program governance structure to provide oversight of its FSM programs and projects. The FSM high-level governance structure includes the following:

- **DHS Under Secretary for Management**, who serves as the acquisition decision authority and approves or rejects program recommendations made by the FSM Executive Steering Committee and the Acquisition Review Board during the Board's meetings. The acquisition decision authority is responsible for ensuring program compliance with DHS acquisition policies by approving program advancement into each phase of the acquisition program process.
- **Acquisition Review Board**, which is the departmental executive board that reviews certain acquisition programs for executable business strategy, resources, management, accountability, and alignment to strategic initiatives. The board also supports the acquisition decision authority in determining the appropriate direction for the program at acquisition decision events.
- **FSM Executive Steering Committee**, which serves as a decision-making body to provide strategy and department-level direction; approves the prioritization, scope, and timing of component modernization plans; and makes formal program recommendations to the DHS Under Secretary for Management.
- **Component Acquisition Executive**, who is the senior acquisition official within the component. The component acquisition executive has responsibility to review, oversee, and direct acquisition program management activities for programs, including the FSM programs. The component acquisition executive is a member of the FSM and solution executive steering committees.
- **Office of the Chief Financial Officer - JPMO**, which is the primary point of contact for all FSM activities. The office leads cross-collaboration and provides project management, oversight, and governance for FSM efforts.

- **Other line of business executive steering committees (e.g., asset, procurement, etc.)**, which are responsible for identifying and communicating FSM issues and concerns to FSM Executive Steering Committee members, as well as providing strategic and tactical guidance to help ensure program success.
- **Solution executive steering committees**, which are program-level decision-making bodies that review and approve requirements, implementation strategies, schedules, and risk management documentation and provide recommendations to the FSM Executive Steering Committee. The FSM-Trio, FSM-FEMA, and FSM-Cube programs each have their own solution executive steering committee.
- **Current working groups**, which review and provide feedback on FSM documentation and monitor and provide governance to support FSM Executive Steering Committee decisions.
- **Integrated project teams**, which JPMO leads and serve as the interface between JPMO and the components. Integrated project teams are composed of representatives from appropriate functional disciplines, including component subject matter experts, and are responsible for performing tasks needed to achieve program and project goals.
- **Component project teams**, which perform day-to-day management of component FSM project execution and serve as component-level project management offices and integrated project teams. They are composed of component subject matter experts and execute tasks, report status updates, and write FSM program documents.

See figure 1 for an outline of DHS's tiered FSM governance structure.

Figure 1: Department of Homeland Security's Tiered Financial Systems Modernization Governance Structure

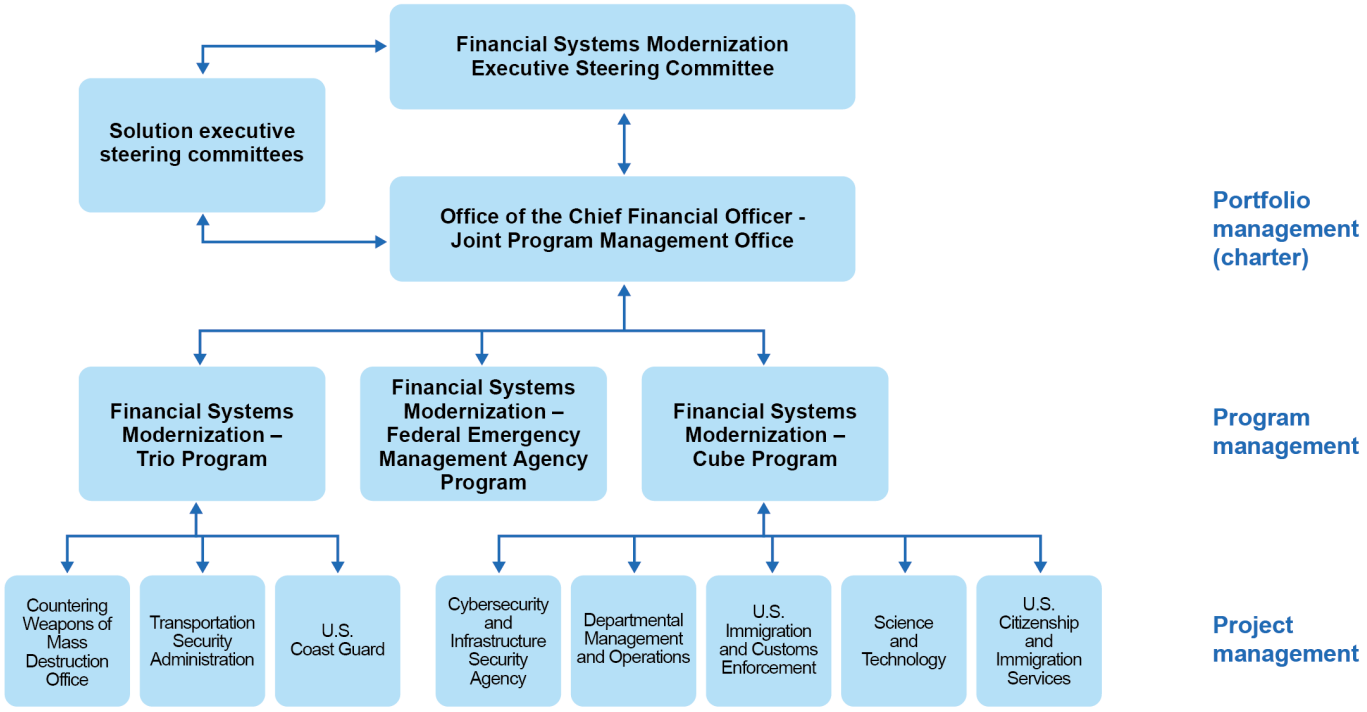


Source: GAO analysis of DHS documentation. | GAO-23-105194

JPMO is to provide the FSM Executive Steering Committee with regular status updates and receives direction from the committee regarding FSM efforts. If JPMO reaches an impasse on any decisions, recommendations, or approaches, it is to elevate the item to the FSM Executive Steering Committee or to the appropriate solution executive steering committee for resolution. Figure 2 is a high-level diagram showing the oversight

structure JPMO uses to manage the multiple FSM programs and component projects.

Figure 2: Joint Program Management Office Oversight Structure for Financial Systems Modernization Programs



Source: GAO analysis of Department of Homeland Security documentation. | GAO-23-105194

The JPMO oversight structure includes the following:

- **Portfolio management.** JPMO manages the portfolio of FSM programs across the department by providing an enterprise vision for the future as well as guidance, standardization, and controls in FSM processes.
- **Program management.** JPMO oversees development and implementation of FSM programs, including supporting the identification and selection of solutions, and procures software, integration, and other support services for FSM programs. FSM-Trio,

FSM-FEMA, and FSM-Cube are designated as major acquisition programs under DHS acquisition policy.[16]

- **Project management.** Some FSM programs may have multiple component offices included in the program. For example, FSM-Trio includes CWMD, TSA, and Coast Guard. JPMO oversees the individual component projects within each program and interfaces with the components at the project management level through the integrated project teams. These teams are responsible for performing tasks needed to achieve FSM goals, coordinating with other teams as needed to complete the tasks, and communicating tactical decisions from JPMO to the components and other stakeholders.

In addition to the FSM program governance structure described above, DHS has established policies and processes for managing major acquisition programs, which the FSM programs must follow.[17] DHS policy establishes that a major acquisition program's decision authority review the program at a series of predetermined acquisition decision events to assess whether the major program is ready to proceed through the acquisition life cycle phases. This review is conducted at the Acquisition Review Board meetings.

An important aspect of acquisition decision events is the acquisition decision authority's review and approval of key documents. These documents include the program's acquisition program baseline, which is the agreement between the acquisition program, component, and department-level officials that establishes how the system being acquired will perform, when it will be delivered, and the cost. Specifically, the acquisition program baseline establishes a program's schedule and key performance parameters (KPP). DHS requirements policy describes KPPs as a program's most important and nonnegotiable requirements that a system must meet to fulfill its fundamental purpose.

The acquisition program baseline establishes objective (target) and threshold (latest acceptable for schedule, maximum acceptable for cost, and minimum or maximum acceptable for performance) baselines.

[16]DHS defines major acquisition programs as those with life cycle cost estimates of $300 million or more. In some cases, DHS may define a program with a life cycle cost estimate less than $300 million as a major acquisition if it has significant strategic or policy implications for homeland security, among other things.

[17]See Department of Homeland Security, *Acquisition Management Directive*, DHS Directive 102-01, Rev. 1.3 (Feb. 25, 2019), and *Acquisition Management Instruction*, DHS Instruction 102-01-001 (Jan. 21, 2021).

According to DHS policy, if a program fails to meet any schedule, cost, or performance threshold approved in the established baseline, it is considered to be in breach. A program in breach status is required to notify its acquisition decision authority and develop a remediation plan that outlines a time frame for the program to pursue one of three options: (1) return to its established baseline parameters; (2) establish a rebaseline with new schedule, cost, and performance goals; or (3) have a DHS-led program review that recommends a revised baseline. For more information on the DHS major acquisition process and life cycle, see appendix IV.

Joint Concept of Operations

DHS has developed a *Joint Concept of Operations* (J-CONOPS), which documents DHS's high-level plans to modernize and integrate its financial, procurement, and asset management systems and business processes for its FSM efforts.[18] The J-CONOPS describes deficiencies or capability gaps with the current way of operating and explains how different solutions could meet future challenges and correct current shortfalls. The J-CONOPS, along with the *Joint Operational Requirements Document*, provides a bridge between the top-level capability needs spelled out in the mission need statement and the detailed technical requirements found in the performance specifications. The final version of the J-CONOPS demonstrates the preferred solution or solutions and is validated by DHS's Joint Requirements Council.[19]

FSM Enterprise Capability Gaps

According to the J-CONOPS, DHS needs the capability to report on financial management, procurement, and asset management functions to comply with applicable statutes, regulations, and directives and for management's decision-making purposes at the department and component levels. DHS components separately defined their FSM capability gaps and mission needs in a set of mission need statements. The component-specific capability gaps were synthesized into 10 enterprise capability gaps in the J-CONOPS. Current FSM enterprise capability gaps described in the J-CONOPS are shown in table 1.

[18]Department of Homeland Security, *Joint Concept of Operations for Financial Systems Modernization (J-CONOPS),* Version 2.0 (July 18, 2022).

[19]The DHS Joint Requirements Council oversees the DHS requirements generation process, harmonizes efforts across the department, and makes prioritized recommendations to the Deputy's Management Action Group for those validated requirements.

Table 1: Financial Systems Modernization Enterprise Capability Gaps That DHS Identified

Gap #	Capability gap	DHS description of capability gap
1	Data management	Legacy systems require manual adjustments to transaction-level data (e.g., journal vouchers and top-side adjustments) that create data integrity risks and potential audit risks. Compensating controls are in place but require significant staff time and resources. These issues also lead to agency financial management systems not complying substantially with the *U.S. Standard General Ledger* at the transaction level, as required by the Federal Financial Management Improvement Act of 1996. Discrepancies between data stored in multiple systems cause issues and require manual reviews and reconciliations.
2	Insufficient security and internal controls	The security and internal controls that the legacy systems employ are insufficient and difficult to manage. This issue is primarily due to the lack of access control, configuration management, and segregation of duties role-based user assignments. As a result, manual compensation controls are used, which increases audit risk.
3	Lack of integrated financial systems	Legacy systems do not effectively or efficiently integrate or interface with required internal and external systems that have a financial impact, requiring numerous manual processes and work-arounds. This issue includes entering data and transactions into multiple systems manually. The manual processes increase the risk of poor data integrity, are inefficient and ineffective, and do not facilitate a paperless work environment.
4	Restricted legacy system flexibility and reporting capabilities	The legacy environments' inflexibility inhibits effective and efficient use of financial analysis and reporting tools. DHS customers must routinely resort to nonstandard methods to respond to financial information requests and produce reports requested by DHS, the Office of Management and Budget, Congress, etc. This issue prevents DHS from obtaining information timely and efficiently to support critical decisions.
5	Absent or impaired integrated business systems capability	DHS lacks the ability to streamline financial data collection and sharing across the enterprise. DHS relies on manual, labor-intensive data calls to generate department-level financial reports. The department lacks the capability to share information across organizational boundaries and from disparate systems.
6	Inability to adapt to emerging requirements	Some legacy systems cannot adapt to anticipated and emerging requirements without additional customization and work-arounds. Some financial systems require numerous system changes and enhancements to preserve functionality, meet changing or new requirements from DHS and authoritative sources, or correct system issues.
7	Lack of an open system	Legacy system proprietary constraints contribute to a closed system environment with limited web services and application programming interfaces. This constraint reduces optimal access to and understanding of system structure. These limitations impair flexibility and limit resources available to enhance performance and improve operational support.
8	Limited capability to support DHS efforts to standardize systems, data, and processes	Legacy operations restrict DHS's ability to fully support its efforts to evolve financial systems management governance policy and standards to ultimately achieve the capability to standardize data and operational processes.
9	Noncompliance with federal regulation and accounting standards	Current systems do not fully comply with government-wide financial and accounting requirements and guidance for timely, reliable, and accurate accounting. There is inconsistent reporting from financial systems that do not comply with *U.S. Standard General Ledger* and DHS accounting classification structure. Inconsistent standards and processes from manual entries are required for nonintegrated systems.
10	Lack of real-time enterprise view of resources across DHS	DHS lacks the capability to share information across organizational boundaries and from disparate systems. Data standardization efforts, that is use of modernized financial systems combined with use of business intelligence tools, can provide an enterprise view of resource use across DHS.

Source: Department of Homeland Security (DHS) documentation. | GAO-23-105194

Component-Specific Capability Gaps

In 2013, Coast Guard stated that its legacy financial management system, the Core Accounting System (CAS), did not comply with government accounting standards and requirements. According to Coast Guard's mission need statement, CAS was a highly customized version of Oracle Federal Financials involving numerous modifications to the software.[20] This caused the inability to readily modify the CAS suite and forced Coast Guard to rely on nonstandard business processes, work-arounds, and extensive compensating controls to counteract the deficiencies and weaknesses caused by the customizations.

Further, according to Coast Guard, the customizations, deferred maintenance, and limited ability to make system fixes effectively put CAS in jeopardy of catastrophic failure. According to Coast Guard, the primary goal of acquiring its new financial management system was to integrate the financial, contract, and asset accountability functions, as well as improve system operational performance to meet user needs. CAS is no longer Coast Guard's financial management system because it was replaced with FSMS in December 2021.

According to FEMA's mission need statement, its current operational environment consists of separate financial, asset, and acquisition management systems. Specifically, the integration between these systems is inefficient and often requires manual processes.[21] This creates challenges in management reporting, thereby limiting FEMA leadership's ability to understand in a timely manner how all resources, including financial resources, are being employed to support decision-making. According to the mission need statement, the current FEMA financial management system, known as the web Integrated Financial Management Information System, uses an application for which FEMA has difficulty obtaining operation and maintenance services.

[20]According to Coast Guard's mission need statement, Coast Guard identified seven capability gaps: (1) noncompliance with federal regulations, (2) manual reconciliation of incompatible data sets, (3) inability to meet new requirements, (4) inefficiency and system failure risk, (5) limited capability to integrate business systems, (6) risks of procurement law violations and protests, and (7) IT controls.

[21]According to FEMA's mission need statement, FEMA identified five capability gaps: (1) lack of integration; (2) operational inefficiency; (3) lack of system flexibility; (4) inability to consistently produce accurate, relevant, and timely data; and (5) system vulnerability to cyber-security threats.

Further, the web Integrated Financial Management Information System has security weaknesses, requires significant manual processes, and possesses poor reporting functionality. According to FEMA, these shortcomings led to increased costs and reduced responsiveness in carrying out its mission.

According to ICE's mission need statement, its current financial system is affecting its ability to effectively and efficiently meet mission objectives and support the DHS mission.[22] ICE uses the Federal Financial Management System and provides financial management and reporting services to the U.S. Citizenship and Immigration Services (USCIS), Science and Technology Directorate (S&T), Cybersecurity and Infrastructure Security Agency (CISA), and Departmental Management and Operations (DMO). According to DHS, the current system has insufficient security controls and inhibits effective and efficient use of financial analysis and reporting tools.

Further, the current system does not effectively or efficiently integrate or interface with internal and external systems requiring the manual recording of transactional information. The system also cannot adapt to emerging requirements without additional customization and work-arounds. Finally, according to DHS, ICE's current system has proprietary constraints that reduce optimal access to and understanding of system structure.

FSM Standard Business Processes

The J-CONOPS describes the nine standard end-to-end financial business processes aligned to the functional areas of core financial, procurement, asset management, and business intelligence reporting. The goal of the FSM standardized business processes is to support implementation of common data sets, improve data quality, and reduce the amount of rework necessary to pass audit checks intended to improve the efficiency of operations and reduce costs. The nine FSM standard business processes that DHS identified are as follows:

1. **Budget formulation to execution.** Includes the full life cycle from budget formulation through final budget execution, including all aspects of budget reporting.

[22]According to ICE's mission need statement, ICE identified the following seven capability gaps: (1) data integrity, (2) legacy system internal security controls, (3) restricted legacy system flexibility, (4) absence or impaired integrated business systems capability, (5) inability to adapt to emerging requirements, (6) lack of open system, and (7) limited capability to support the department's federated structure.

2. **Record to report.** Encompasses establishing and maintaining general ledger master data, recording transactions, account validation rules, accounting period maintenance, reconciliation of data, and managerial and legally required financial reports.
3. **Request to procure.** Consists of activities for procurement through contracts and travel, training, and bank card purchases.
4. **Procure to pay.** Encompasses receiving and accepting goods or services, invoice processing, disbursing payments, payment follow-up, modifying and closing out an obligation, and reporting.
5. **Bill to collect.** Comprises accounts receivable and debt management activities.
6. **Reimbursable management.** Encompasses establishing, maintaining, reconciling, and closing out reimbursable agreements between federal or nonfederal customers.
7. **Cost management.** Consists of defining, measuring, analyzing, and accumulating costs using a consistently applied methodology to clearly align expenses to the programs supported.
8. **Acquire to dispose.** Includes actively managing assets throughout their life cycle, from acquisition to operations maintenance and then disposal.
9. **Business intelligence and decision-support reporting.** Encompasses using business intelligence, which includes using data management technologies to provide information from trends and events, and reporting for enhanced predictive analysis and decision-making.

JPMO-Level and Program-Specific Plans to Implement Modernization Efforts

DHS has both JPMO-level and program-specific plans to implement modernization efforts. The JPMO-level plans focus on the overall financial system modernization approach for DHS, while the program-specific plans address the specific component modernization programs and projects.

JPMO-Level FSM Plans

JPMO has FSM strategies and a program management plan that describe the overall modernization approach for DHS and provide a framework to define the program activities, responsibilities, and timing of events. It leads DHS FSM efforts from acquisition through program execution and sustainment, and provides centralized program governance and streamlined decision-making for the FSM efforts.

JPMO's approach for the FSM efforts includes three key elements: (1) investing in financial management systems modernization for those components with the greatest business need, (2) leveraging business process reengineering to create a full set of standard processes that can be used across DHS to the maximum extent possible, and (3) expanding business intelligence and standardizing data across components to quickly provide enterprise-level reporting. DHS plans for its new financial management system to have a federated architecture. Meaning FSM-Trio, FSM-FEMA, and FSM-Cube may all implement unique financial management systems but use the same financial accounting standards, data standards, and reporting standards. Each FSM program will conduct systems integration in accordance with a common set of enterprise-wide requirements along with component-specific requirements.

According to program officials, JPMO executes and manages two types of contracts for the FSM efforts: software and systems integration support. For software, components can select from three available vendors, each representing software for commercially available off-the-shelf software that meets JPMO's requirements.[23] Program officials stated that the software options have out-of-the-box functionality and will be configured for component-specific requirements by the systems integrator. For systems integration support, components can select from seven available vendors that provide systems integration, program management, operations and maintenance, services desk, and training support.

In November 2022, DHS awarded contracts for software licenses for both FSM-FEMA and FSM-Cube, according to DHS officials. Officials also said that the FSM-Trio program contract was originally structured differently, with the program starting under a federal shared service provider. Then in 2018, the FSM-Trio program moved from the federal shared service provider to DHS's data center, transferring the systems modernization work to DHS. According to DHS officials, DHS is currently transitioning FSM-Trio to a new contract for system integration support services and stated that it plans to award contracts for system integration services for FSM-FEMA and FSM-Cube.

[23]Under the Federal Acquisition Regulation, a commercially available off-the-shelf item refers to any item of supply that is a commercial product; sold in substantial quantities in the commercial marketplace; and offered to the U.S. government, under a contract, in the same form that it is sold in the commercial marketplace. 48 C.F.R. § 2.101(b).

Coast Guard's FSM Plan and Deployment

Coast Guard, the third of the FSM-Trio components, deployed its new financial management system, FSMS, in December 2021.[24] DHS missed its original planned date of October 2020 because it could not conduct cutover and go-live for both TSA and Coast Guard.[25] The Coast Guard go-live was rescheduled for October 2021; however, this date was further delayed to December 2021 primarily due to data migration issues.

DHS planned to declare full operational capability for FSMS in late calendar year 2022. However, because of known system issues and deficiencies identified in follow-on testing and reported in the *System Evaluation Report* issued in September 2022, DHS declared a breach of program baselines. As a result, DHS postponed the declaration of full operational capability of FSMS at Coast Guard.[26] According to a JPMO official, the program office is developing a remediation plan and will provide it to the Acquisition Review Board in the second quarter of fiscal year 2023 for approval.

Coast Guard was included in an *FSM-Trio 2021 Life Cycle Cost Estimate*, which DHS updated with actual costs where available. The total cost estimate for the FSM-Trio program for fiscal years 2018 through 2025 is $510 million. Of the total estimated cost, $248 million is for implementation costs funded by DHS headquarters; $156 million is for operations and maintenance costs funded by Coast Guard; and the remaining amount is funded by CWMD, TSA, and JPMO.

FEMA and ICE FSM Plans

Both FEMA and ICE are in the planning phases of their FSM efforts to acquire software and systems integration services. Each component has developed a unique program management plan for its FSM program. The FSM-FEMA program management plan, dated April 2022, defines the relationship of the FEMA program management office and JPMO, and

[24]FSMS is a suite of off-the-shelf Oracle federal financial management applications. FSMS system modules include Oracle Federal Financials, Oracle business intelligence enterprise edition/Oracle business intelligence application (OBIEE/OBIA), and MarkView. OBIEE/OBIA is used for reporting purposes, and MarkView is used for invoice routing and approval as well as property management capabilities.

[25]Cutover, also called migration, is the period of time when data are migrated into the new solution and the legacy system is turned off.

[26]According to DHS guidance, a program breach must be declared when a key performance parameter is not met upon the completion of the operational test and evaluation. Specifically, a breach occurs when a program or project fails to meet any cost, schedule, or performance threshold in the approved acquisition program baseline.

details the approach for program execution, monitoring, and control during the acquisition life cycle.

According to DHS, the department decided to delay the acquisition processes in the first quarter of fiscal year 2020 for FSM-FEMA and FSM-Cube because of a bid protest filed by a prospective offeror before the U.S. Court of Federal Claims. The court denied the protest in the first quarter of fiscal year 2021.[27] A separate bid protest challenging the agency's subsequent contract awards was filed in the U.S. Court of Federal Claims in the fourth quarter of fiscal year 2021, and was denied by the court in the second quarter of fiscal year 2022.[28] According to a JPMO official, in mid-November 2022, DHS awarded contracts for software licenses for both FSM-FEMA and FSM-Cube. However, in late November 2022 DHS received a bid protest filed with GAO pertaining to this award that the protestor withdrew in January 2023.

The FSM program management plan for ICE and its customers, dated May 2022, established how JPMO, in partnership with component program management offices, will coordinate the management of the FSM-Cube program. The plan also describes the program's management practices intended to support compliance with DHS policies and the success of the FSM-Cube implementations.

DHS officials stated that the FEMA and ICE financial management systems solutions will integrate financial, procurement, and asset management systems. However, no specific cost estimates and detailed program schedules are available at this point because DHS is still in the process of awarding contracts for the systems integrator for each project. DHS's fiscal year 2023 budget request includes $12 million for FSM at FEMA. Further, ICE requested $10.6 million for procurement, construction, and improvements funding related to FSM-Cube. JPMO officials expect to develop full life cycle cost estimates in the second or third quarter of fiscal year 2023.

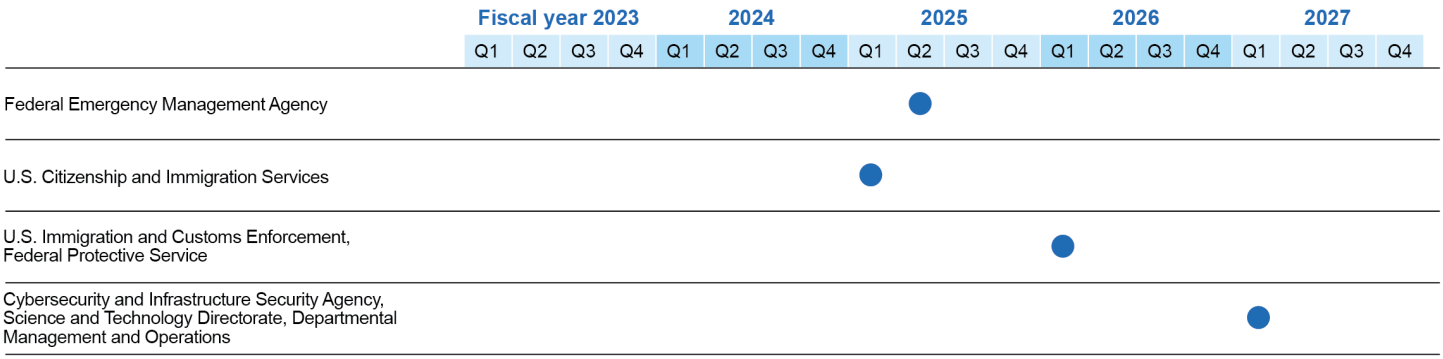
FEMA is currently estimated to go live in the second quarter of fiscal year 2025. The current notional go-live schedule for the FSM-Cube program

[27]See *Savantage Financial Services, Inc. v. United States,* 150 Fed. Cl. 307 (Oct. 16, 2020).

[28]See *Savantage Financial Services, Inc. v. United States,* 158 Fed. Cl. 240 (Feb. 23, 2022). A post-award bid protest is a written objection filed by a government contractor that is challenging a federal agency's award of a contract for procuring property or services.

estimates USCIS going live in the first quarter of fiscal year 2025, with ICE and Federal Protective Service following in the first quarter of fiscal year 2026.[29] The final ICE customers, CISA, S&T, and DMO, are scheduled to go live in the first quarter of fiscal year 2027. Figure 3 depicts DHS's estimated schedule for FEMA and ICE implementations, as well as other selected components, as of September 2022.

Figure 3: Initial Go-Live Dates (Subject to Revision) for Selected Financial System Modernization Programs and Components (as of September 2022)



Source: GAO analysis of Department of Homeland Security documentation. | GAO-23-105194

Lessons Learned from FSM Efforts

JPMO has established a process and continues to document and consider lessons learned from both the current FSM efforts and past financial management system modernization attempts. The *FSM JPMO Lessons Learned Standard Operating Procedures* define a lesson learned as knowledge or understanding gained by work experience that has a significant impact or benefit to the project or program. Lessons learned comprise good practices and improvement opportunities and are documented in a lessons learned register.

- **Good practice.** A lesson learned observation or experience that has shared learning value for what went well, such as best practices performed or noteworthy event successes, and is to be continued and shared appropriately.
- **Improvement opportunity.** An identified issue or pain point that can be improved by determining and removing its root cause and planning

[29]The ICE customer, DMO, is responsible for certain financial activities for the Federal Protective Service, under the Management Directorate.

and taking applicable corrective actions to improve future performance.

According to DHS officials, the lessons learned process starts after completing a major program event. Major program events include when the system goes live or technical refreshes occur. DHS officials stated the Business Transformation Branch schedules lessons learned meetings with each functional area. The team has a general set of areas that it addresses in each meeting, including budget, planning, risk, communication, best practices, what went well, and what did not go well. The team is to document sessions in meeting notes and consolidate lessons into a lessons learned register database after meetings.

Stakeholders are to review and analyze the lessons learned gathered during scheduled lessons learned meetings or following the meetings using the FSM lessons learned register. DHS officials explained that the key points are summarized in a lessons learned report, which includes actions for components to consider to help them achieve future project goals more smoothly. The report is to summarize the lessons into several overarching themes that address every phase of the project. The lessons learned included in the report are intended to provide actionable guidance to mitigate the risk of repeating the same lessons. The last step is to implement process improvement opportunities, during which lessons learned owners monitor and implement corrective actions.

Lessons Learned from Past and Current Modernization Efforts

DHS has a register that lists 127 lessons learned from past and current financial systems modernization programs. Table 2 shows these 127 in the high-level categories defined by DHS.

Table 2: Number of Financial Systems Modernization (FSM) Lessons Learned by Category from 2004 through 2022

Category	Total
Change management and organizational change management	**25**
Systems engineering	**18**
Training	**17**
Cloud or data management/migration	**10**
Governance	**9**
Cost	**8**
Schedule	**7**
Scope	**6**
Testing/defect management	**6**

Category	Total
Communications	5
Human resources	5
Program/project management	4
Quality	3
Risk and risk management	2
No category	2
Total	**127**

Source: Department of Homeland Security documentation as of June 2022. | GAO-23-105194

JPMO's organizational change management team coordinated and facilitated information-gathering sessions focused on four important events or phases associated with the Coast Guard's FSMS modernization effort: organizational change management, training, data migration, and testing.

Organizational change management. JPMO identified 10 lessons learned and the following three main themes:

- Accurately understanding the business processes to help ensure that end users understand how the new solution will affect them.
- Fully understanding the new solution so that organizational change management activities can accurately portray how it will affect end users.
- Effectively communicating and championing system changes to earn the respect and trust of their leadership and peers.

Training. JPMO identified 17 lessons learned and three main themes:

- Tailor training to the component's business processes and emulate the actual work environment.
- Ensure users' roles and responsibilities are effectively mapped, so they can enroll in the appropriate role-based training classes.
- Offer training earlier and give users opportunities to practice both to enhance their skills and to mitigate learning degradation.

Cloud or data management migration. JPMO identified 10 lessons learned and four main themes:

- User acceptance testing must be completed prior to cutover, since defects not addressed in user acceptance testing will affect cutover and go-live.
- Failure to execute data cleansing will significantly affect data migration.
- Mock data migration events need to clarify how business processes are to work for key areas such as capital projects and reimbursable accounting.
- The manual cutover financial system tool must be tailored to the component's needs.

Testing. JPMO identified six lessons learned and two main themes:

- More time must be devoted to testing, particularly user acceptance testing. According to the Coast Guard lessons learned report, failure to conduct accurate and comprehensive testing results in issues or challenges that will be carried over into cutover and go-live.
- More subject matter experts (SME) need to be allocated to accomplish testing objectives, and SMEs need to be fully invested and not have to maintain their regular duties during testing.

In addition, FSM program officials stated that there were two critical lessons learned from the Coast Guard go-live decision. The first was that JPMO needs to ensure that components have an alternative financial system to process transactions. FSM program officials explained that this could be an issue in the future with FEMA. Specifically, FEMA will likely have to invest funds in its current legacy system to ensure that it will be available in case the acquisition of a modernized system does not move forward as planned.

The second critical lesson learned, according to program officials, was that JPMO cannot rely exclusively on one go-live date at year-end. In future FSM efforts, JPMO will ensure that contingency plans are in place to ensure that system conversion does not affect the ability to make critical payments on time. This includes ensuring that legacy systems are available to continue with operations and developing strategies for a midyear cutover should outstanding issues prevent cutover at the beginning of a fiscal year.

FSM-FEMA and FSM-Cube Implementation of Past Lessons Learned

According to DHS officials, the FSM-FEMA and FSM-Cube programs consider lessons learned from past and current modernization efforts. DHS officials stated that a standard practice to ensure lessons learned

are an active part of the FSM implementation program is to include a requirement to consider lessons learned in the FSM-FEMA and FSM-Cube program charters. According to DHS, lessons learned are shared with upcoming FSM programs through project meetings. FSM program officials stated that JPMO has briefed FSM-FEMA and FSM-Cube program management on lessons learned from the implementation of FSMS. For example, officials suggested FSM-FEMA and FSM-Cube (1) consider including key performance parameters (KPP) in the scope of work, (2) provide training on an ongoing basis and ensure appropriate staff attend training, and (3) identify SMEs and ensure that they have time to devote to system testing.

DHS officials stated that FSM-FEMA and FSM-Cube used a change readiness analysis tool early on and have compared the results to the lessons learned to craft messaging and other avenues of information sharing. DHS officials also stated that the FSM-FEMA and FSM-Cube organizational change management integrated project teams have reviewed lessons learned. These will be incorporated into their strategies.

DHS Has Not Yet Fully Achieved Expected Capabilities for Coast Guard's FSMS Implementation

DHS's JPMO identified, documented, and tracked metrics to assess the deployment of FSMS, Coast Guard's new financial management system. However, Coast Guard is not realizing all of the expected capabilities from the implementation of FSMS because of serious issues identified in system testing that have not been resolved.

DHS Identified Metrics and Milestones for FSM Efforts

DHS's JPMO identified and documented a number of metrics and milestones that focus on business and operational user requirements, including KPPs. The metrics JPMO tracks cover seven key requirement areas: system reliability, system availability, system maintainability, system effectiveness, system restoration, data restoration, and reliability.

JPMO communicated the status of these metrics to Coast Guard stakeholders in various meetings, such as monthly FSM Executive Steering Committee meetings, monthly FSM-Trio Executive Steering Committee meetings, and the weekly Operations & Maintenance (O&M)

meetings.[30] For example, DHS communicated detailed statuses on a range of key metrics and KPPs to specific component program managers and executive staff during these periodic meetings. JPMO briefed the steering committee members on high-level milestones and development progress. Finally, the O&M meetings covered more granular O&M activities, achievements, metrics, and general status updates.

Consistent with federal laws,[31] guidance,[32] and best practices,[33] management should ensure that as a project continues to develop, the project continues to meet mission needs as expected and delivers operational functions related to the business requirements. If the project is not meeting expectations or if problems arise, management should ensure that the necessary corrective actions are taken to address the deficiencies. Further, according to federal guidance and best practices, objectives for measurement and analysis techniques should be specified and aligned with information needs for the project. To do so, management should ensure that the processes for measuring performance are established and used consistently over time. Specifically, these processes should

1. identify and document metrics to measure outcomes of the program;
2. establish baseline and milestone measures for current state performance metrics;
3. define success targets expected to be achieved after completion of the program;

[30]Executive Steering Committee meetings changed from monthly to quarterly after the May 2021 meeting, starting with the August 2021 meeting.

[31]31 U.S.C. § 3512(c), (d), commonly referred to as the Federal Managers' Financial Integrity Act; FFMIA; and the Information Technology Management Reform Act of 1996, Pub. L. No. 104-106, div. D-E, 110 Stat. 186, 679-703 (Feb. 10, 1996), as amended by Pub. L. No. 104-208, div. A, tit. VIII, § 808, 110 Stat. 3009-393-94 (Sept. 30, 1996), also known as the Clinger-Cohen Act of 1996.

[32]Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular No. A-130 (July 2016).

[33]See Software Engineering Institute, *CMMI® for Acquisition,* vrs. *1.3* (Nov. 2010); Project Management Institute, Inc., *The Standard for Program Management*, 4th edition (Newtown Square, Pa.: 2017); General Services Administration, *Modernization and Migration Management (M3) Playbook*, accessed Feb. 2, 2021, https://www.ussm.gov/m3; and GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590G (Washington, D.C.: Sept. 2020).

4. monitor performance and milestones for the new system and processes; and
5. report the results to relevant stakeholders to inform management decisions, identify areas for improvement, and take appropriate corrective action.

When management follows these processes, management can more effectively monitor the progress of a project, determine whether the expected operational capabilities are being delivered as intended, and proactively take corrective action as needed.

JPMO identified and documented key metrics, business processes, and system requirements for FSMS in the J-CONOPS and the *Joint Operational Requirements Document* (J-ORD). For example, the J-CONOPS documents the shared requirements for DHS's financial management systems modernization efforts. The J-CONOPS describes the modernized financial management systems in terms of the user needs it must fulfill, as well as the relationship with existing systems and business processes. The J-ORD establishes and documents KPPs, which are operational requirements determined by the DHS user community. It also establishes that failure to meet a KPP threshold (the minimum achievable level of operational performance to satisfy the mission needs) would result in a program breach. The J-ORD organizes the KPPs into four key areas:

1. **System effectiveness:** The ability of the system to provide timely and accurate transactional process results to the user when the system is under high demand for system resources.
2. **System responsiveness:** The ability of the system to provide timely data analytics and query process results to the user.
3. **Data restoration:** The ability of the system to provide restored capability from a catastrophic loss or data disruption from solution operations to include corruption, destruction, loss, and compromise of the system.
4. **System reliability:** The probability that the solution will not fail during 24 hours of operation.

In addition to developing the KPPs, JPMO and the FSM-Trio components—including Coast Guard—developed and monitored program schedules for the implementation of key milestones throughout the FSM-Trio program. Executive Steering Committee members discussed both the status of KPPs as well as the schedules at the various steering

committee meetings throughout the implementation of FSMS at Coast Guard. For example, the monthly FSM-Trio Executive Steering Committee meetings discussed the status of the implementation of FSMS against both KPPs and key milestone dates. These items were also discussed at the Acquisition Review Board meetings.

Coast Guard Is Not Yet Fully Achieving Expected Capabilities from FSMS Implementation

While JPMO and Coast Guard identified, measured, and tracked a number of key metrics as noted above, Coast Guard is not realizing all of the expected capabilities from the implementation of FSMS. Serious issues identified in operational system testing will need to be resolved before system capabilities are fully realized.

According to the J-ORD, an FSM program reaches initial operational capability when the program has (1) operational and integrated financial management, (2) procurement and asset management capabilities that fully support the designated mission-essential functions as defined in the J-CONOPS, and (3) successful completion of applicable testing events. Prior to declaring initial operational capability, the following conditions should be met, among others:

- all mission-essential activities are fully supported;
- migration of mission-essential documents from legacy systems to the new system is complete, tested, and accurate; and
- applicable user testing is developed and complete.

Further, the J-ORD stipulates that for full operational capability to be achieved, an FSM program should meet the following conditions, among others: (1) the new system is deployed to all components within the FSM program, (2) the new system is integrated with all DHS and component standard business processes, and (3) operational and evaluation testing is complete and the new system is operating effectively. If a program does not meet one or more of the approved thresholds, then the program manager is to declare that a program breach occurred. When there is a program breach, the program manager is to prepare a remediation plan, which discusses the options considered and the rationale for the proposed corrective action recommendation.

While noting concerns about the system, DHS declared initial operational capability for FSMS. Specifically, in a June 2022 memorandum, DHS declared the initial operational capability for FSMS at Coast Guard. However, this memorandum stated that Coast Guard management was

"extremely concerned about the integration, functionality, and future sustainment" of FSMS. The memorandum summarized the criteria for initial operational capability, as documented in the J-ORD and the status of meeting operational requirements, based on testing results.

The memorandum indicated that most mission-essential activities and a majority of the system interfaces were operational, but each of these activities needed additional work prior to full operational capability status. For example, the memorandum stated that there were significant challenges remaining in the areas of financial reporting and funds management. Specifically, contract documents would become trapped in automated workflows and manual corrections to records had to be made for Coast Guard to continue processing contract awards.

According to the memorandum, user testing was deemed sufficient; however, the memorandum noted issues related to the system's reporting capabilities. For example, the memorandum stated that (1) not all user acceptance testing was finalized, (2) FSMS did not have reliable or consistent reporting capabilities, and (3) Coast Guard's ability to accurately monitor budget execution tasks was at risk. Although known issues remained, a risk-based consensus decision was made to go live during the production readiness review.

DHS subsequently conducted follow-on operational testing and evaluation to support full operational capability for FSMS. The testing was performed on FSMS for key metrics from May 2022 through June 2022, and the results were documented in the *System Evaluation Report* (SER) in September 2022.[34] The SER is used to support the approval to deploy the program and declare full operating capability for FSMS, among other things.

According to the SER, three of the four FSM-Trio KPPs that JPMO tracked for implementation did not meet the threshold for passing—

[34]The Transportation Security Administration/Acquisition Program Management/ Operational Test Branch was the designated Joint-Independent Test Agent for this follow-on operational test and evaluation. This testing focused on Coast Guard's implementation of FSMS; however, some data were collected from the other Trio components–TSA and CWMD. For example, all Trio components provided responses to the user experience questionnaire and system usability scale survey. Additionally, the Trio components provided information on the system's cyber resiliency and operations and maintenance reports.

system effectiveness, system responsiveness, and system reliability.[35] The other KPP, data restoration, passed with limitations. The SER concluded that the FSMS system did not support auditability of financial statements and process transactions or provide data analytics in a timely or accurate manner. Therefore, users could not complete their mission tasks effectively.

The SER noted that in addition to a breach at the program level, the users of the system were affected by failed KPPs, and management could not make decisions because of inaccurate information. If the system is not reliable, there is an increased risk that unexpected failures could occur and cause the system to become unavailable, affecting users' ability to complete their daily tasks. The SER recommended, among other things, that JPMO and Coast Guard

- continue to address issues and improve system functionality,
- build a schedule that will maximize the user/SME participation,
- ensure test readiness before the start of testing,
- strengthen the systems' configuration management,
- complete scheduled maintenance outside of normal operation hours to reduce system disruptions to users,
- address concerns Coast Guard reported in the initial operational capability approval memorandum prior to full operational capability decision,
- continue to improve system performance to address latency issues, and
- extend help desk hours to support all system users regardless of geographic location.

As previously discussed, DHS's auditors reported a new material weakness in the audit of the department's fiscal year 2022 financial statements that related to Coast Guard's migration to FSMS. According to the audit report, this system migration resulted in significant changes to existing processes, including changes to the process for recording

[35]In addition to the four KPPs discussed above that JPMO tracked for implementation and reported on in the SER, the SER testing results also included four Coast Guard-specific KPPs. Two related to system design, one related to system performance, and one related to system security controls, along with other Coast Guard system operational requirements.

obligations and expenditures incurred against obligations. Specifically, DHS's auditors found that Coast Guard had insufficient design and implementation of controls over both the review of obligations incurred and recording the receipt of goods and services to ensure the accuracy of expenditure records.

The serious findings discussed above, along with those reported in the fiscal year 2022 financial statement audit report, affect management and stakeholders' ability to rely solely on system-generated reports to prepare accurate and auditable financial statements. The findings also affect Coast Guard's ability to make timely and critical management decisions with assurance. As a result of these serious findings, DHS declared a breach of program baselines for performance and decided to delay its planned December 2022 declaration of full operational capability for FSMS at Coast Guard. DHS expects to deliver a remediation plan to the Acquisition Review Board in the second quarter of fiscal year 2023.

The findings discussed above also mean that users cannot rely on FSMS to complete their assigned duties accurately and timely. The inability to rely on FSMS can have costly consequences, putting DHS and Coast Guard at risk of inaccurate financial reporting, inaccurate budget reporting, and failure to comply with certain legal requirements.

The program breach occurred largely because the agency had not fully addressed serious findings and known issues identified by system testing at Coast Guard and included in the SER. Until JPMO works with Coast Guard to remediate known issues, such as those resulting from testing the system's ability to demonstrate expected operational capabilities, DHS remains at an increased risk that the new system will not meet its mission needs or the requirements defined in the J-ORD.

The Acquisition Review Board is a DHS decision-making body that met throughout the acquisition life cycle process to discuss and evaluate risks with implementing FSMS at Coast Guard. The review board considered various factors to determine whether Coast Guard was ready to move forward with the implementation in December 2021:

- the testing events leading up to the acquisition decision event,
- the status of Core Accounting System (CAS),
- the cutover schedule leading up to the go-live, and
- risks and issues with approving or delaying the go-live decision.

For example, the Deputy Under Secretary for Management determined that the user acceptance testing that occurred from July through September 2021 was "considered inadequate." Specifically, testers only completed 70 percent of the planned tests in the allotted time and identified a number of severe defects. According to the user acceptance testing report, the criteria for completing user acceptance testing were not met.[36] In order for user acceptance testing to be complete, the criteria require that there are no severe defects remaining and known issues have been remediated.

Additionally, the review board considered the possibility of delaying the go-live date; however, the additional time was capped at 6 months because CAS was scheduled to be decommissioned in March 2022. Further, DHS officials told us that continuing to use CAS was not an option because it had a number of vulnerabilities, and DHS was unable to extend the contracted system support. Table 3 summarizes key risks the review board identified and discussed at various meetings.

Table 3: Key Risks the Acquisition Review Board Identified for Coast Guard's Financial Systems Modernization Solution

Risk title	Description of risk	Response strategy
Incomplete testing of interfaces	Comprehensive testing was not performed for all key interfaces, making it likely that Coast Guard users would encounter defects upon go-live that interrupt transaction processing.	Perform procedures to mitigate this risk
Data conversion	The inability to test at least one complete legacy data conversion for all Coast Guard data sets in any of the mock tests makes it likely that issues would surface during the actual data migration, creating cutover schedule delays or data issues upon go-live.	Perform procedures to mitigate this risk
Tight cutover schedule	If there was a delay in specific critical path areas, then there would be a corresponding delay in the go-live date.	Perform procedures to mitigate this risk
No rollback option	If unexpected issues hindered the migration of Coast Guard to the new financial system, then Coast Guard would be without a financial system as there was no readily available alternative to roll back to the prior financial system.	Accept this risk

Source: Department of Homeland Security documentation as of September 2021. | GAO-23-105194

Coast Guard is working on addressing risks and issues identified and discussed above. To help avoid similar risks and issues on future systems modernization efforts for FEMA and ICE, it is essential that DHS perform sufficient testing prior to proceeding to the next phase in the acquisition process. Further, follow-up and resolution of critical deficiencies are critical to successful modernizations. Doing so will help

[36]Department of Homeland Security, Joint Program Management Office, *Trio User Acceptance Test Plan*, version 1.0 (June 28, 2021).

minimize the risks of not delivering modernized systems that can produce reliable data for management decision-making and financial reporting.

Coast Guard's Corrective Action Plans Did Not Always Address Required Attributes

Modernizing components' financial management systems—such as the FSMS implementation at Coast Guard—is one of DHS's key efforts to address issues identified in prior audit findings and address its designated high-risk financial management outcomes. To obtain a clean opinion on internal control over financial reporting, and to help ensure the success of its FSM efforts, DHS must address its existing material weaknesses in IT systems and financial reporting through effective and timely remediation.

To address its fiscal year 2021 audit findings related to IT systems and financial reporting, Coast Guard developed corrective action plans, which generally fall into two categories: (1) mission action plans (MAP) for financial reporting issues and (2) remediation plans or plans of action and milestones (POA&M). However, these plans did not always contain all of the attributes recommended in applicable guidance.

Coast Guard's Fiscal Year 2021 Audit Findings

In fiscal year 2021, DHS's auditors reported material weaknesses in (1) controls over financial reporting and (2) IT controls and information systems, as well as FFMIA noncompliance. System limitations contribute to deficiencies in multiple financial process areas across DHS. Many key DHS information systems do not comply substantially with federal financial management systems requirements as defined by FFMIA. These system limitations increase the risk of error and result in inconsistent, incomplete, or inaccurate information reported to management.

Various control deficiencies at Coast Guard contributed to both of these material weaknesses and to FFMIA noncompliance. Specifically, auditors communicated 32 NFRs for Coast Guard in fiscal year 2021. Twenty-two of the NFRs related to the two material weaknesses in internal control identified in DHS's audit report and two related to a significant deficiency. Twenty-six of the NFRs related to FFMIA noncompliance.[37] However, DHS was able to obtain a clean opinion on its financial statements through significant manual compensating controls.

DHS's auditors also issued NFRs in fiscal year 2021 related to Coast Guard's new financial system, FSMS. While not yet implemented at Coast Guard during fiscal year 2021, FSMS was in use at another DHS

[37]Twenty-two of the 32 NFRs we reviewed were related to both material weaknesses or significant deficiencies and FFMIA noncompliance.

component, TSA. The six consolidated FSMS NFRs related to the DHS IT controls and information systems material weakness and affected all DHS financial statement line items. Issues that auditors identified in these NFRs included ineffective design of audit log review for the application, operating system, and database supporting FSMS; ineffective implementation of POA&Ms; ineffective implementation of authorization to operate requirements; ineffective implementation of account recertification of privileged operating system and database access; and ineffective implementation of policies and procedures over FSMS.

Guidance for Corrective Action Plans

Corrective action plans at Coast Guard generally fall into two categories for control deficiencies: (1) financial NFRs for financial reporting issues, which are to follow DHS and Coast Guard guidance to have MAPs developed to address them, and (2) IT NFRs for IT security control and system weaknesses, which are to follow Department of Defense (DOD) and Coast Guard guidance and have remediation plans or POA&Ms developed to address them.

In accordance with Office of Management and Budget (OMB) guidance and DHS policy, financial NFRs should have corresponding MAPs that are developed, implemented, and managed for all areas where material weaknesses, significant deficiencies, or control deficiency conditions exist.[38] MAPs are to follow the OMB Circular No. A-123 guidance and the DHS MAP guide, both of which have specific guidance on the attributes to include in MAPs.[39] For this report, we will refer to all corrective action plans that follow OMB Circular No. A-123 and DHS MAP guidance as MAPs. These attributes include identification of the root cause, determination of the resources required to correct a control deficiency, and development of critical path milestones needed to resolve the control deficiency. For a full list of the MAP attributes from guidance, see appendix V.

Additionally, for MAPs that are not related to material weaknesses or significant deficiencies, Coast Guard follows guidance created by its Audit Remediation and Property Oversight Division, the *Coast Guard Corrective*

[38]For many of the DHS components, to distinguish better between what is reported to and monitored by the Risk Management and Assurance team versus what is managed internal to the component, a "corrective action plan" is commonly used for any remedial plan not required to be submitted to the Risk Management and Assurance team.

[39]Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control,* OMB Circular No. A-123 (July 15, 2016), and Department of Homeland Security, *Internal Control Mission Action Plan Guide* (2021).

Action Plan Desk Guide. The desk guide contains general guidance on MAP development, approval, execution, monitoring, and completion.

DHS components are responsible for developing and implementing MAPs. For NFRs related to DHS material weaknesses and significant deficiencies, components submit MAPs to DHS's Risk Management and Assurance office for additional review and approval. According to DHS, the Chief Financial Officer (CFO) established the Risk Management and Assurance office to manage the risks, communication, and progress of various financial management activities. These activities include supporting components' efforts to implement the DHS plan for compliance with OMB Circular No. A-123 and establishing a DHS-wide accountability structure and MAP process.

According to Risk Management and Assurance officials, their office reviews submitted MAPs for compliance with DHS guidance. The office verifies that a component performed a root cause analysis and that the corrective action identified would reasonably address the root cause of the deficiency. Additionally, DHS requires components to report the current status of all milestones to the Risk Management and Assurance office each month for all MAPs related to significant deficiencies and material weaknesses.

For any deficiency, including significant deficiencies and material weaknesses, related to an IT control, Coast Guard must follow DOD policies, *U.S. Coast Guard Cybersecurity Policy*, and the POA&M Process Guide, which contain requirements for IT remediation plans, most commonly using the POA&M structure.[40] Since Coast Guard uses some systems that are either connected to or hosted on the DOD Information Network, DHS and DOD agreed that Coast Guard would follow DOD's cybersecurity standards. For IT NFRs related to a Coast Guard system, Coast Guard creates a POA&M in a DOD system used to track them.

Additionally, Coast Guard creates an associated DHS corrective action plan to allow Coast Guard officials to monitor remediation efforts. According to Coast Guard officials, this gives the CFO visibility into

[40]DOD Instruction 8500.01, *Cybersecurity* (Mar. 14, 2014); DOD Instruction 8510.01, *Risk Management Framework for DOD Systems* (July 19, 2022); Coast Guard Commandant Instruction 5500.13G, *U.S. Coast Guard Cybersecurity Policy* (Jan. 25, 2022); and Coast Guard, *Plan of Action and Milestones and Waiver Request Process Guide*, version 4.0 (Jan. 19, 2018).

remediation efforts. If the system is external to Coast Guard, then Coast Guard will develop a corrective action plan and not a POA&M. If DHS has identified an IT NFR or process that needs to be monitored each month, Coast Guard will develop a MAP and not a POA&M.

Data Attributes Missing in About Half of Coast Guard's Corrective Action Plans

Coast Guard developed corrective action plans to address selected fiscal year 2021 NFRs related to material weaknesses, significant deficiencies, and FFMIA noncompliance; however, the plans did not always contain all of the data attributes recommended in guidance. Specifically, eight of 17 corrective action plans we reviewed were missing recommended attributes, including seven of 17 plans that did not indicate that a root cause analysis had been performed.[41] Based on these issues, Coast Guard is at increased risk that its corrective actions will not effectively address identified deficiencies in a timely manner.

We found that Coast Guard did not consistently prepare MAPs in accordance with OMB Circular No. A-123 and DHS and Coast Guard guidance. Specifically, three of seven MAPs did not have a root cause identified and did not determine the resources required to correct a control deficiency. All seven MAPs included critical path milestones needed to resolve the deficiency.

According to the DHS MAP guidance, accurate identification of the root cause is one of the most critical elements of developing an effective MAP that will help to successfully resolve the control deficiency. DHS MAP guidance states root cause analysis should be based on investigation by component MAP officials, since MAPs based on auditor findings alone will often result in weak, incomplete, or misguided remediation efforts.

Generally, the four MAPs addressing material weaknesses and significant deficiencies that the Risk Management and Assurance office reviewed contained the attributes required by OMB and DHS guidance. Specifically, the DHS MAP Guide identifies 28 attributes to include in significant deficiency and material weakness-related component MAPs, which include an issue description, root cause, key performance measures, resources required, milestone topic, and status. The four MAPs related to material weaknesses or significant deficiencies contained 111 of 112 (99 percent) of the attributes identified.

[41]We reviewed 17 corrective action plans, which included seven MAPs and 10 POA&Ms for 17 NFRs related to material weaknesses, significant deficiencies, or FFMIA noncompliance.

Three MAPs related to FFMIA noncompliance that were managed at the Coast Guard component level, without Risk Management and Assurance office oversight, contained significantly fewer MAP attributes. The *Coast Guard Corrective Action Plan Desk Guide* identifies 18 attributes to include in component MAPs not related to significant deficiencies or material weaknesses. These three MAPs had 21 of 54 (39 percent) of attributes identified in the Coast Guard guidance. None of the three FFMIA-related control deficiency MAPs had a root cause identified or determined the resources required to correct the deficiency, as required by OMB Circular No. A-123. Missing these attributes puts Coast Guard at an increased risk that its corrective actions may not effectively address identified deficiencies related to FFMIA noncompliance in a timely manner.

When asked about the attributes missing from the MAPs, Coast Guard officials did not explain why specific attributes identified in OMB Circular No. A-123 and Coast Guard guidance were missing from the three FFMIA-related control deficiency MAPs we reviewed. Coast Guard officials stated that they only followed the DHS MAP guidance for MAPs related to material weaknesses and significant deficiencies, not for other types of control deficiencies. Coast Guard officials stated that they use the *Coast Guard Corrective Action Plan Desk Guide* for MAPs not related to significant deficiencies or material weaknesses, which takes into account OMB Circular No. A-123 requirements, including conducting a root cause analysis and determining the resources required to correct a control deficiency.

We reviewed POA&Ms for 10 IT NFRs related to material weaknesses and FFMIA noncompliance. We found that Coast Guard did not consistently prepare them in accordance with applicable guidance. Of the 19 Coast Guard IT NFRs selected for analysis, nine did not have corresponding POA&Ms, for various reasons. Coast Guard did not address the seven CAS-related NFRs because that system would no longer be in use following the transition to FSMS. For two of the NFRs, Coast Guard did not create POA&Ms because the NFRs related to external information systems that Coast Guard did not own. Instead, Coast Guard created corrective action plans to track the status of these control deficiencies. According to Coast Guard officials, the system owner is responsible for any remediation actions related to external information systems.

Four of the 10 POA&Ms we reviewed were missing at least one of the six attributes identified in the POA&M guide, including not identifying the root

cause of the vulnerability. Additionally, three of the 10 POA&Ms did not identify resources needed to resolve the vulnerability. All 10 POA&Ms identified actions and activities needed to resolve the vulnerability, developed at least one milestone, developed a timeline for resolution, and recorded vulnerabilities and a remediation strategy. Table 4 summarizes the results of our evaluation of Coast Guard POA&Ms against applicable guidance.

Table 4: Evaluation of Coast Guard Plans of Action and Milestones (POA&M) Against Guidance

Key attribute	Number of POA&Ms with required attribute (out of 10 reviewed)
Determine the root cause of the vulnerability	6
Identify actions and activities needed to resolve the vulnerability	10
Identify resources needed to resolve the vulnerability	7
Develop at least one milestone	10
Develop a timeline for resolution	10
Record vulnerabilities and remediation strategy in the POA&M	10

Source: GAO analysis of Department of Homeland Security documentation. | GAO-23-105194

According to Coast Guard officials, Coast Guard recently updated its POA&M Process Guide as of September 1, 2022. These officials stated that the updated guide provides an approach for Coast Guard to remediate or mitigate risks in accordance with Coast Guard priorities and DOD policies. It also contains screenshots and updated guidance on how to process POA&Ms in Coast Guard's current POA&M management system. Coast Guard officials explained that the current POA&M management system is in the process of being updated to reflect the required fields documented in the recent POA&M Process Guide.

When asked about the attributes missing from the POA&Ms reviewed, Coast Guard officials acknowledged that some of the POA&Ms were missing root cause analyses and may not have included adequate data for the resources field. Specifically, Coast Guard officials stated that root cause analyses are performed using a separate template and the finished root cause analyses are uploaded into Coast Guard's POA&M management system and saved separately. For some of the POA&Ms, these analyses were not created and uploaded into the system.

According to Coast Guard officials, the new POA&M Process Guide will alleviate some of the confusion related to performing and documenting root cause analyses. Coast Guard officials further stated that all POA&Ms had data filled out for the resources field, but acknowledged that the data may not adequately identify resources for each required item. Incomplete corrective action plans increase the risk that Coast Guard's corrective actions may not effectively address identified deficiencies in a timely manner.

Conclusions

DHS is executing a multiyear plan to implement modern financial management systems at three of its components that contribute to its inclusion on GAO's High Risk List: Coast Guard, FEMA, and ICE. JPMO and Coast Guard identified, documented, and tracked a number of metrics and milestones to measure and monitor the success of the implementation of FSMS at Coast Guard. However, Coast Guard has not fully realized the expected capabilities of the implementation of FSMS because of serious issues identified in its system testing. Until JPMO works with Coast Guard to remediate these issues, risks are increased that the new system will not meet its mission needs or expected capabilities. Sufficient testing and follow-up on identified deficiencies will also be key to reducing the risks to FEMA and ICE modernizations.

DHS has taken some actions to remediate audit findings and address its high-risk financial management outcomes at Coast Guard. However, corrective action plans did not always include all of the data attributes recommended in guidance, such as assuring that root cause analyses were performed. Including all applicable data attributes and identifying the root cause of deficiencies in corrective action plans could help Coast Guard ensure that plans lead to effective remediation of issues.

Recommendations for Executive Action

We are making the following four recommendations to DHS:

DHS's Under Secretary for Management should ensure that the Joint Program Management Office works with Coast Guard to remediate known issues identified from testing, prior to declaring full operational capability for the ongoing financial systems modernization efforts. (Recommendation 1)

DHS's Under Secretary for Management should ensure that the Joint Program Management Office works with FEMA to remediate issues as they arise from user testing prior to moving forward with subsequent milestones for the ongoing financial systems modernization efforts. (Recommendation 2)

DHS's Under Secretary for Management should ensure that the Joint Program Management Office works with ICE to remediate issues as they arise from user testing prior to moving forward with subsequent milestones for the ongoing financial systems modernization efforts. (Recommendation 3)

DHS's Under Secretary for Management should ensure that Coast Guard follows applicable guidance when developing corrective action plans to include documenting the root cause analysis and other recommended attributes. (Recommendation 4)

Agency Comments

We provided a draft of this report to DHS for review and comment. In written comments, reproduced in appendix VI, the department concurred with our four recommendations and described actions it has taken and will take to address the issues we identified with its FSM program and Coast Guard's corrective action plans. Those actions, if implemented as described, should address our recommendations. The department also provided technical comments on our report that we incorporated as appropriate.

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

If you or your staff have any questions about this report, please contact me at (202) 512-9816 or rasconap@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 members who made key contributions to this report are listed in appendix VII.

Paula M. Rascona
Director
Financial Management and Assurance

Appendix I: Objectives, Scope, and Methodology

The objectives of this report were to (1) describe the Department of Homeland Security's (DHS) oversight and management of its financial systems modernization (FSM) efforts, modernization plans at selected components, and lessons learned from past and current FSM efforts; (2) examine the extent to which DHS has achieved expected capabilities for the U.S. Coast Guard's newly deployed financial management system; and (3) examine the extent to which DHS has taken actions to address certain audit findings related to financial reporting and IT system weaknesses.

To address our first objective, we met with DHS officials to discuss current governance structure and oversight procedures as well as the current financial management systems environment at Coast Guard, Federal Emergency Management Agency (FEMA), and U.S. Immigration and Customs Enforcement (ICE). We reviewed DHS's descriptions and plans for the future financial management systems environments at these three components.

To further enhance our understanding of DHS's governance and oversight procedures over the Joint Program Management Office (JPMO) and component executive steering committees, we reviewed key documentation, including (1) DHS's *Financial Systems Modernization Governance Strategy and Approach*; (2) the *DHS FSM JPMO Charter* dated April 2019; (3) the DHS Deputy Under Secretary for Management's March 6, 2019, memorandum *Department of Homeland Security Financial Systems Modernization Programs: Progress and Key Tenets for the Path Forward*; and (4) the *Financial Systems Modernization Roadmap* dated October 2018.

Regarding DHS's current and planned future financial systems environments at Coast Guard, FEMA, and ICE, we reviewed each component's mission need statement, the *Joint Concept of Operations* (J-CONOPS), and J-CONOPS addenda for FEMA and ICE.[1] To describe DHS's modernization strategies and program management plans, including cost and schedule at Coast Guard, FEMA and ICE, we reviewed the following: (1) the *Financial Systems Modernization Roadmap*, (2) *FSM-Trio 2021 Life Cycle Cost Estimate Update*, (3) *FSM JPMO Program*

[1]DHS refers to the FSM program for ICE and its customers as FSM-Cube. The FSM-Cube program includes ICE, Cybersecurity and Infrastructure Security Agency, Departmental Management and Operations, Science and Technology Directorate, and U.S. Citizenship and Immigration Services.

Management Plan (PMP), (4) *FSM-FEMA PMP*, (5) *FSM-Cube PMP*, and (6) relevant acquisition decision event decision memos.[2]

To describe the FSM lessons learned process and identify the lessons learned from prior FSM initiatives and the current implementation of the new financial management system at Coast Guard, we reviewed (1) the *FSM JPMO Lessons Learned Standard Operating Procedure*, (2) the *DHS FSM Coast Guard Lessons Learned* report, and (3) lessons learned register. We reviewed the lessons learned register and summarized lessons learned by status, category, and source project, as identified by DHS. We also met with DHS officials to discuss modernization plans and lessons learned.

To address our second objective, we met with DHS officials to gain an understanding of DHS and Coast Guard's process for identifying, measuring, and tracking key metrics for Coast Guard's new financial management system. We reviewed documentation of the metrics used to assess the expected capabilities and the implementation status of the Financial Systems Modernization Solution (FSMS) at Coast Guard. Specifically, we reviewed the following DHS documentation: (1) *Joint Operational Requirements Document*; (2) J-CONOPS; (3) *DHS Trio User Acceptance Test Plan* dated June 28, 2021, as well as test results dated February 15, 2022; (4) *Follow-On Operational Test Plan for FSMS – Trio Supporting the U.S. Coast Guard Release* dated April 13, 2022; (5) operations and maintenance status meetings from January 2021 to August 2022; (6) FSM and Trio Executive Steering Committee meetings from January 2021 to May 2021; (7) key Acquisition Review Board meeting minutes from November 2019 to December 2021; and (8) the *System Evaluation Report* issued September 28, 2022.

Further, to identify relevant criteria we reviewed leading practices and federal guidance related to metrics and processes for measuring expected capabilities. These documents included (1) OMB Circular No. A-130, *Managing Information as a Strategic Resource*; (2) Software Engineering Process Management Program, *CMMI® for Acquisition*; (3) Project Management Institute Inc., *The Standard for Program Management*; (4) DHS's *Agile Guidebook*; (5) General Services

[2]The following three DHS components are included in the FSM-Trio program: Countering Weapons of Mass Destruction Office, Transportation Security Administration, and Coast Guard.

Administration's *Modernization and Migration Management (M3) Playbook*; and (6) prior GAO work.[3]

To assess JPMO's process for measuring expected capabilities for deploying Coast Guard's new financial management system against leading practices and federal guidance, we reviewed DHS's documentation of the process that JPMO took to identify, track, and assess FSMS metrics and to make decisions on how to conduct data migration from Core Accounting System, the legacy system, and from Cutover Financial System to FSMS. We compared JPMO's process for deploying Coast Guard's FSMS against leading practices and federal guidance we identified.

To address our third objective, we reviewed relevant guidance documents, including (1) Office of Management and Budget (OMB) Circular No. A-123; (2) the Risk Management and Assurance *Internal Control Mission Action Plan (MAP) Guide*; (3) Department of Defense (DOD) Instruction 8500.01 *Cybersecurity*; (4) DOD Instruction 8510.01, *Risk Management Framework for DOD Systems*; (5) *Coast Guard Corrective Action Plan Desk Guide*; and (6) Coast Guard's *Plan of Action and Milestones (POA&M) and Waiver Request Process Guide*, version

[3]Office of Management and Budget, *Managing Information as a Strategic Resource,* OMB Circular No. A-130 (July 2016); Software Engineering Process Management Program, *CMMI® for Acquisition*, vrs. 1.3 (Nov. 2010); Project Management Institute, Inc., *The Standard for Program Management*, 4th edition (Newtown Square, Pa.: 2017), and Department of Homeland Security, Office of the Chief Technology Officer, *Agile Guidebook* (Dec. 31, 2020). GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590G (Washington, D.C.: Sept. 2020), and General Services Administration, *Modernization and Migration Management (M3) Playbook*, accessed Feb. 2, 2021, https://www.ussm.gov/m3; along with prior GAO work, including GAO, *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, GAO-05-927 (Washington, D.C.: Sept. 9, 2005); *Information Security: Concerted Effort Needed to Improve Federal Performance Measures*, GAO-09-617 (Washington, D.C.: Sept. 14, 2009); and *Managing for Results: Government-wide Actions Needed to Improve Agencies' Use of Performance Information in Decision Making*, GAO-18-609SP (Washington, D.C.: Sept. 5, 2018).

4.0.[4] We also met with DHS and Coast Guard officials to discuss both the MAP and POA&M processes at DHS and Coast Guard.

To identify the relevant corrective action plans related to material weaknesses, significant deficiencies, and agency financial management systems' substantial noncompliance with requirements of the Federal Financial Management Improvement Act of 1996 (FFMIA) (referred to as FFMIA noncompliance for purposes of this report), we obtained copies of all 32 fiscal year 2021 notices of findings and recommendations (NFR) issued for Coast Guard and also obtained six consolidated NFRs that related to FSMS.[5] We reviewed the NFRs and cross-walked the NFRs to the DHS fiscal year 2021 referenced financial report exhibits to determine which were related to material weaknesses and significant deficiencies. We also reviewed the NFRs to determine which NFRs related to FFMIA noncompliance, as indicated by DHS's financial auditors within the NFRs.

Of the 32 fiscal year 2021 NFRs, we did not request corrective action plans for four Coast Guard financial NFRs because they did not relate to material weaknesses, significant deficiencies, or FFMIA noncompliance. Of the remaining 28 NFRs, 24 Coast Guard NFRs (five financial and 19 IT) related to material weaknesses and significant deficiencies, and four additional financial NFRs related to financial management systems' substantial noncompliance with FFMIA requirements.

We analyzed five Coast Guard financial NFRs and 19 IT NFRs related to material weaknesses and significant deficiencies, and four additional financial NFRs related to FFMIA noncompliance. We requested corrective action plans to address these 28 NFRs. However, we did not analyze corrective action plans for 11 of the 28 NFRs for various reasons. No corrective action plan was developed to address one of the FFMIA-related financial NFRs and seven of the IT NFRs. According to Coast

[4]Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control,* OMB Circular No. A-123 (July 15, 2016); Department of Homeland Security, *Internal Control Mission Action Plan Guide* (2021); DOD Instruction 8500.01, *Cybersecurity* (Mar. 14, 2014); DOD Instruction 8510.01, *Risk Management Framework for DOD Systems* (July 19, 2022); Coast Guard Commandant Instruction 5500.13G, *U.S. Coast Guard Cybersecurity Policy* (Jan. 25, 2022); and Coast Guard, *Plan of Action and Milestones and Waiver Request Process Guide*, version 4.0 (Jan. 19, 2018).

[5]We reviewed the most recent results of the fiscal year 2022 financial statement audit report to update the background for this report, provide additional context throughout the report, and monitor the status of DHS high-risk issues. However, we did not obtain the NFRs or corrective action plans for fiscal year 2022 because those were issued too late to be included in the scope of this audit objective.

Guard officials, they had not yet created a MAP for the financial NFR because additional time was needed for users to understand FSMS, the new Coast Guard financial system, before creating a MAP for this deficiency. Coast Guard officials further stated that they did not address seven NFRs related to the Coast Guard legacy financial system because that system would no longer be in use following the transition to FSMS. Additionally, one financial NFR was related to an IT material weakness, so Coast Guard followed different guidance than for the rest of the financial NFR MAPs and it was not reviewed. Further, two IT NFRs related to external information systems that Coast Guard did not own. According to Coast Guard officials, the system owner is responsible for any remediation actions related to external information systems, so we did not evaluate corrective action plans related to these NFRs.

As a result, we obtained 17 relevant corrective action plans and evaluated the corrective action plans (7 MAPs and 10 POA&Ms) against OMB, DHS, DOD, and Coast Guard guidance to determine the extent to which corrective action plans addressed auditor findings. Specifically, we reviewed whether Coast Guard included required data attributes in the corrective action plans, such as identification of the root cause of deficiencies, the resources required to resolve deficiencies, and milestones for correcting deficiencies. We also obtained remediation plans for the six consolidated NFRs related to the FSMS system, which we summarized but did not include in our corrective action plan analysis as they were not Coast Guard corrective action plans.

We conducted this performance audit from March 2021 to February 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Financial Management Actions and Outcomes for Addressing High-Risk Areas

Since it was created in 2003, the Department of Homeland Security (DHS) has been on GAO's High Risk List because it had to transform 22 agencies, several with major management challenges, into one department. In 2013, we narrowed the scope of the high-risk area to strengthening and integrating DHS management functions, including financial management. Based on our current review of DHS efforts, we determined that DHS has made progress related to improving its financial management and fully addressing two of the eight high-risk financial management actions and outcomes: (1) obtaining an unmodified (clean) audit opinion on its financial statements and (2) doing so for 2 consecutive years.

However, a significant amount of work is to be completed on the remaining six high-risk financial management actions and outcomes. Table 5 shows our assessment of DHS's progress toward addressing the eight high-risk financial management actions and outcomes as of November 2022.

Table 5: Department of Homeland Security (DHS) High-Risk Financial Management Actions and Outcomes

DHS financial management actions and outcomes	Status of high-risk financial management actions and outcomes (as of November 2022)
Outcome No. 1: Obtain an unmodified (clean) audit opinion on all financial statements.	**Fully addressed.** DHS obtained its first clean opinion on its financial statements in fiscal year 2013.
Outcome No. 2: Obtain an unmodified (clean) audit opinion on internal control over financial reporting (ICOFR) to demonstrate effective internal controls.	**Partially addressed.** DHS has received an adverse opinion on ICOFR for 10 consecutive years—fiscal years 2013 through 2022—and has reduced the number of material weaknesses from 10 in 2006 to four in 2022. However, DHS needs to resolve two long-standing material weaknesses—one in financial reporting and one in IT systems and controls—as well as two new material weaknesses in insurance liabilities and obligations incurred, in order to obtain a clean opinion on ICOFR. DHS is executing a multiyear plan to achieve a clean ICOFR opinion by fiscal year 2024. However, modernizing DHS financial management systems will be key to addressing the material weakness in IT systems and controls.
Outcome No. 3: Sustain unmodified opinions for at least 2 consecutive years on financial statements.	**Fully addressed.** DHS has received an unmodified (clean) audit opinion on its financial statements for 10 consecutive years—fiscal years 2013 through 2022.
Outcome No. 4: Sustain unmodified opinions for at least 2 consecutive years on ICOFR.	**Initiated.** DHS has received an adverse opinion on ICOFR for 10 consecutive years—fiscal years 2013 through 2022—and has reduced the number of material weaknesses from 10 in 2006 to four in 2022. However, DHS still needs to resolve two long-standing material weaknesses—one in financial reporting and one in IT systems and controls—as well as two new material weaknesses in insurance liabilities and obligations incurred, in order to obtain a clean opinion on ICOFR. DHS anticipates making substantial annual progress and continues to build upon its internal control enterprise approach, demonstrating incremental and sustainable progress each year, and remains collectively focused on the fiscal year 2024 target to obtain its first clean opinion on ICOFR and the second in fiscal year 2025.

DHS financial management actions and outcomes	Status of high-risk financial management actions and outcomes (as of November 2022)
Outcome No. 5: Achieve substantial compliance with the Federal Financial Management Improvement Act of 1996 (FFMIA), as reported annually by its independent auditors in accordance with the act.	**Partially addressed.** The U.S. Coast Guard, Federal Emergency Management Agency (FEMA), and U.S. Immigration and Customs Enforcement (ICE) financial management systems do not comply substantially with FFMIA requirements. DHS has launched a multiyear financial systems modernization program to help ensure substantial compliance with FFMIA requirements, and anticipates this outcome being fully addressed in fiscal year 2024. However, DHS does not expect to implement new financial management systems at FEMA and ICE until after 2024.
Outcome No. 6: Effectively manage the implementation of a financial management system solution or modernization of existing systems for the U.S. Coast Guard.	**Partially addressed.** Coast Guard implemented its new Financial Systems Modernization Solution in December 2021. However, in September 2022, DHS reported that the new system was not effective, suitable, or reliable and that it still needs to address known issues with the new system. DHS anticipated reaching full operational capability in December 2022. However, it has been delayed as a result of serious issues with the new system.
Outcome No. 7: Effectively manage the implementation of a financial management system solution or modernization of existing systems for the Federal Emergency Management Agency (FEMA).	**Initiated.** FEMA has begun the procurement process to select software and integration service providers. According to a DHS official, DHS awarded a contract for software license in mid-November 2022 and still plans to award a contract for systems integration services. Following those awards, DHS will conduct a discovery process with the software vendors and integrators. FEMA anticipates going live on the new system in the second quarter of fiscal year 2025.
Outcome No. 8: Effectively manage the implementation of a financial management system solution or modernization of existing systems for the U.S. Immigration and Customs Enforcement (ICE).	**Initiated.** ICE has begun the procurement process to select software and integration service providers. According to a DHS official, DHS awarded a contract for software license in mid-November 2022 and still plans to award a contract for systems integration services. Following those awards, DHS will conduct a discovery process with the software vendors and integrators. ICE anticipates going live on the new system in the first quarter of fiscal year 2026.

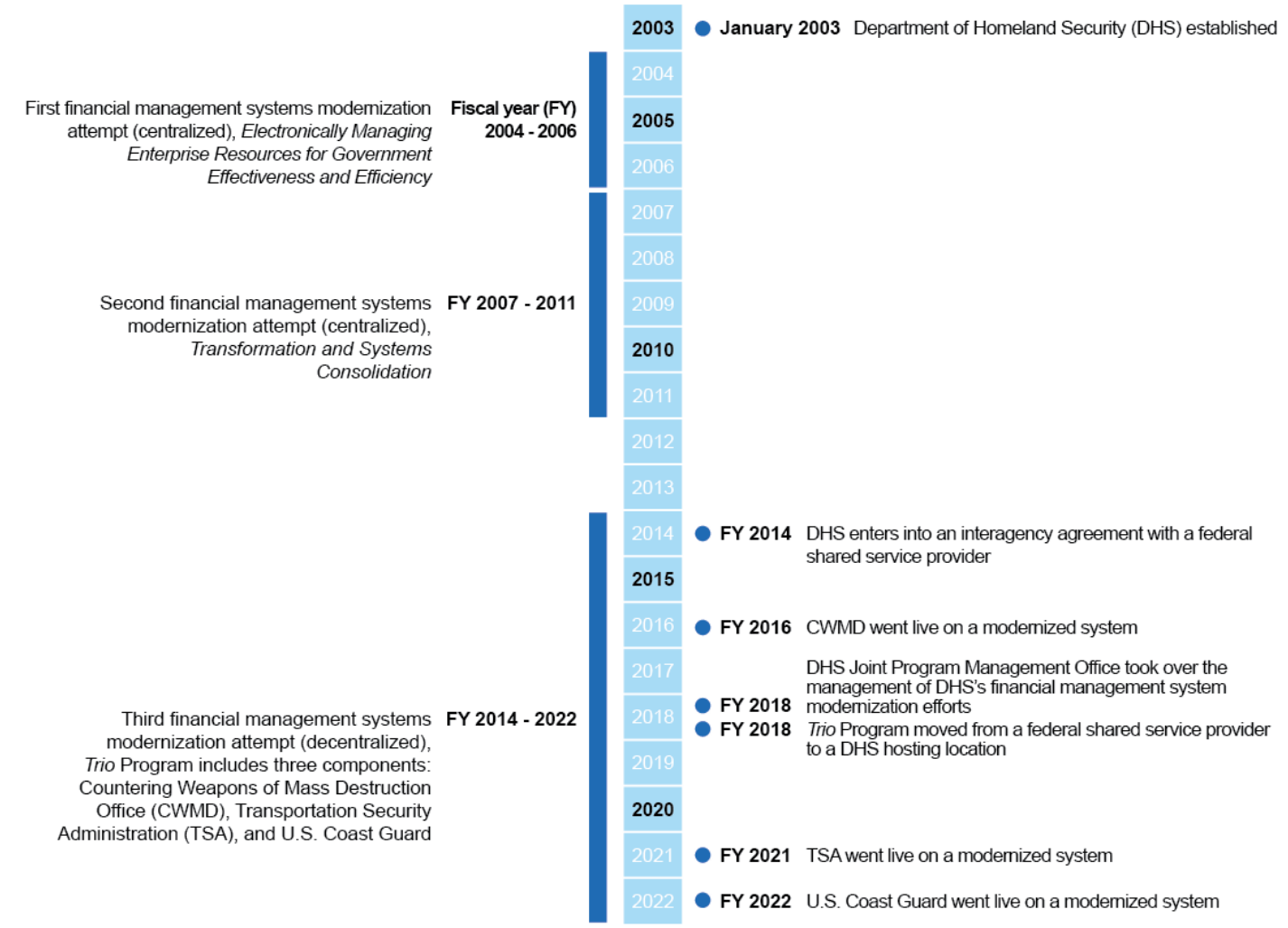
Legend: Fully addressed = Outcome is fully addressed. Mostly addressed = Progress is significant and a small amount of work remains. Partially addressed = Progress is measurable, but significant work remains. Initiated = Activities have been initiated to address the outcome, but it is too early to report progress.

Source: GAO analysis of DHS documentation as of November 2022. | GAO-23-105194

Appendix III: Past Financial Management System Modernization Efforts

The Department of Homeland Security (DHS) has had several initiatives to develop a department-wide integrated and comprehensive financial management system. Past attempts have included the Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency program variations and the Transformation and Systems Consolidation effort, which both focused on implementing a centralized, department-wide system. Figure 4 shows a timeline of DHS's prior attempts to modernize its financial management systems.

Figure 4: Timeline of Department of Homeland Security's Attempts to Modernize Its Financial Management Systems



Source: GAO analysis of DHS documentation. | GAO-23-105194

In 2014, following its second unsuccessful modernization attempt, DHS resumed its financial systems modernization (FSM) efforts using a decentralized, component-level approach. In August 2014, DHS and the U.S. Department of the Interior's Interior Business Center signed an interagency agreement to provide DHS financial system implementation support to three DHS components: Countering Weapons of Mass Destruction Office, Transportation Security Administration, and U.S. Coast Guard—known as FSM-Trio.[1]

The purpose of the FSM-Trio program was to implement a shared service solution enabling these components to perform financial, procurement, and asset management activities.[2] However, DHS determined that Interior could not deliver a viable financial management systems solution that met DHS's requirements. Therefore, in fiscal year 2018, DHS established a Joint Program Management Office to oversee DHS's current FSM efforts at the component level, and the FSM-Trio program transitioned from the Interior Business Center hosting solution to DHS's data center.

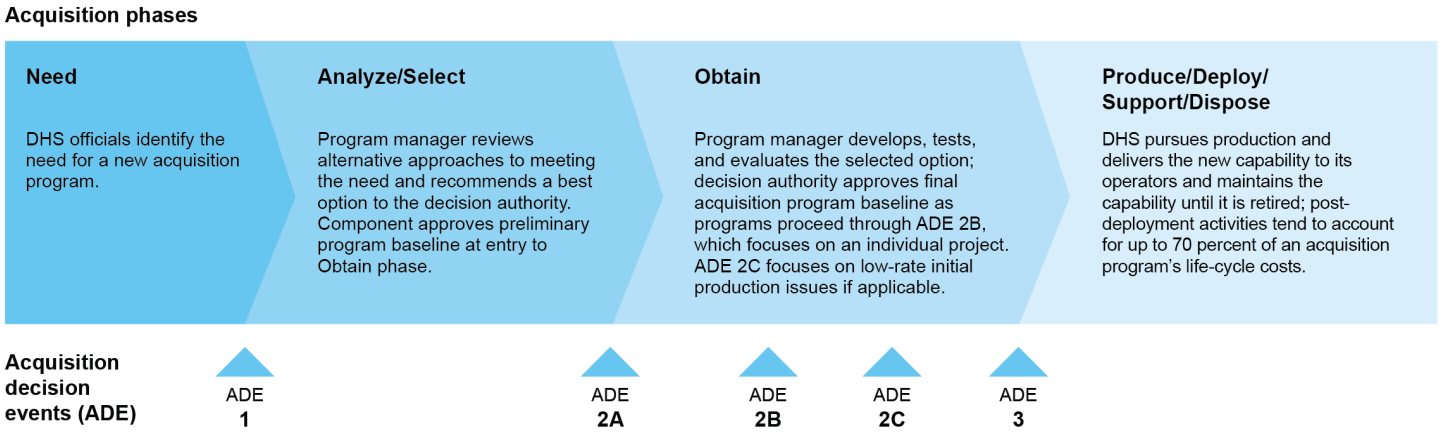
[1]The Domestic Nuclear Detention Center was renamed the Countering Weapons of Mass Destruction Office.

[2]DHS uses nine standard business processes to support four financial management systems capabilities: core financial, procurement (acquisition management), asset management, and business intelligence.

Appendix IV: Major Acquisition Process and Life Cycle

The Department of Homeland Security (DHS) has established policies and processes for managing major acquisition programs,[1] which the financial systems modernization (FSM) programs must follow.[2] DHS policy establishes that a major acquisition program's decision authority should review the program at a series of predetermined acquisition decision events (ADE) to assess whether the major program is ready to proceed through the acquisition life cycle phases. This review is conducted at the Acquisition Review Board meetings. For the FSM programs, the senior official performing the duties of the Deputy Under Secretary for Management is the acquisition decision authority. The acquisition life cycle includes four phases—Need, Analyze/Select, Obtain, and Produce/Deploy/Support/Dispose. Figure 5 reflects the current acquisition life cycle in DHS acquisition management policy.

Figure 5: DHS Acquisition Life Cycle for Major Acquisition Programs



Source: GAO analysis of Department of Homeland Security (DHS) data. | GAO-23-105194

The Need phase focuses on (1) defining the need as it aligns to strategic DHS direction, (2) identifying how DHS currently meets the specific mission and objectives, (3) establishing a high-level view of the desired

[1]DHS defines major acquisition programs as programs with life cycle cost estimates of $300 million or more. In some cases, DHS may define a program with a life cycle cost estimate less than $300 million as a major acquisition if it has significant strategic or policy implications for homeland security, among other things.

[2]Department of Homeland Security, *Acquisition Management Directive*, DHS Directive 102-01, Rev. 1.3 (Feb. 25, 2019), and *Acquisition Management Instruction*, DHS Instruction 102-01-001 (Jan. 21, 2021).

state and mission requirements, and (4) capturing the operational gap against the current state. During this phase, the Joint Requirements Council reviews and validates the mission need statement.[3] The first ADE (ADE 1) is to validate needs. One of the entrance criteria for ADE 1 is determining whether an acquisition program is the appropriate solution by means of a validated mission need statement.

ADE 1 initiates the Analyze/Select phase activities. The Analyze/Select phase identifies and explores alternatives for filling validated user mission capability gaps in the mission need statement with mission effective, suitable, resilient, and affordable solutions. This phase also allows decision makers to select the optimal solution or solutions to effectively deliver the required capability to users. During this phase, the concept of operations and analysis of alternatives documents are completed and an alternative is selected and approved. Once the alternative has been selected, the operational requirements document and acquisition program baseline are finalized. The requirements document also identifies high-level key performance parameters (KPP) that constitute the operational requirements of the selected alternative.

The next event in the process (ADE 2A) is to approve the acquisition program. This approval initiates Obtain phase activities. The Obtain phase develops, tests, and evaluates the preferred alternative selected in the previous phase and prepares it for the Produce/Deploy/Support/ Dispose phase. The Obtain phase also includes preliminary production efforts. The program baseline is approved, which includes subsections laying out the cost, schedule, and performance parameters for each project. This baseline approval takes place during the event known as ADE 2B. In ADE 2C, program management will approve low-rate production or incremental delivery as the next part of the Obtain phase. For the Coast Guard modernization, the ADE 2C decision initiated the approval for Joint Program Management Office to execute go-live activities and migrate Coast Guard from its legacy financial system to the new Financial Systems Modernization Solution.

The next event (ADE 3) is to produce and deploy program products. Based on successful test and evaluation reports, production readiness, sustainment reviews, and verification of sufficient production and operational resources (staffing and funding), the acquisition decision

[3]The DHS Joint Requirements Council oversees DHS's requirements generation process, harmonizes efforts across the department, and makes prioritized recommendations to the Deputy's Management Action Group for those validated requirements.

authority may authorize initiation of the Produce/Deploy/Support/Dispose phase of the acquisition program via ADE 3. During the Produce/Deploy/Support/Dispose phase, the program manager oversees the production efforts and coordinates the transition activities required to fully deploy the capability.

An important aspect of an ADE is the acquisition decision authority's review and approval of key acquisition documents. These documents include the program's acquisition program baseline, which consists of agreements between the acquisition program, component, and department-level officials that establish how systems being acquired will perform, when they will be delivered, and what they will cost. Specifically, the baseline establishes a program's schedule, costs, and KPPs. DHS requirements policy describes KPPs as a program's most important and nonnegotiable requirements that a system must meet to fulfill its fundamental purpose.

The acquisition program baseline establishes objective (target) and threshold (maximum acceptable for cost, latest acceptable for schedule, and minimum or maximum acceptable for performance) baselines. According to DHS policy, if a program fails to meet any schedule, cost, or performance threshold approved in the baseline, it is considered to be in breach. A program in breach status is required to notify its acquisition decision authority and develop a remediation plan that outlines a time frame for the program to either return to its baseline parameters; rebaseline, that is, establish new schedule, cost, or performance goals; or have a DHS-led program review that results in recommendations for a revised baseline.

Appendix V: Summary of Mission Action Plan Attributes from Guidance

Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, states that correcting control deficiencies is an integral part of management accountability and must be considered a priority by the agency. Further, effective remediation of control deficiencies is essential to achieving the objectives of 31 U.S.C. § 3512(c), (d), commonly referred to as the Federal Managers' Financial Integrity Act. The corrective action process provides the mechanism for management to present a comprehensive plan for addressing the risk identified. OMB Circular No. A-123 includes attributes that a corrective action plan requires, including performing a root cause analysis of the deficiency. These attributes apply to mission action plans (MAP) for all control deficiencies.

Additionally, the Department of Homeland Security (DHS) has two sets of internal guidance that apply to the U.S. Coast Guard's MAPs. The *Internal Control Mission Action Plan Guide* applies to all deficiencies identified as material weaknesses or significant deficiencies. The *Coast Guard Corrective Action Plan Desk Guide* applies to control deficiencies that are not material weaknesses or significant deficiencies, but are related to the Federal Financial Management Improvement Act of 1996. Both of these guides outline the procedures used to develop MAPs, as well as recommended attributes MAPs should include. The DHS MAP guide includes 28 attributes and the *Coast Guard Corrective Action Plan Desk Guide* includes 18 attributes.

The attributes required by both OMB Circular No. A-123 and DHS internal guidance documents are listed in table 6.

Table 6: Summary of MAP Data Attributes from Guidance

Guidance attribute	Which MAPs guidance applies
OMB Circular No. A-123	All control deficiency MAPs.
1. Perform root cause analysis	
2. Determine the resources required to correct a control deficiency	
3. Include critical path milestones that affect the overall schedule and performance of the corrective actions needed to resolve the control deficiency	
DHS *Internal Control Mission Action Plan Guide*	Material weakness and significant deficiency-related MAPs.
1. Outline number	
2. Related summary of aggregated deficiencies reference	
3. Related business process risk and control objectives	
4. Fraud risk remediation	
5. Milestone topic	
6. Assessment verification and validation milestone	
7. Control deficiency category	
8. Open start date	
9. Open due date	
10. Open critical milestone	
11. Status	
12. Responsible party/assignee	
13. Assigned	
14. Responsible organization	
15. Project	
16. Open process	
17. Source of control deficiency	
18. Issue description	
19. Financial statement assertions	
20. Mission link	
21. Root cause	
22. Key strategies	
23. Key performance measures	
24. Verification and validation	
25. Risks, impediments, and dependencies	
26. Dependencies to other MAPs	
27. Resources required	
28. Audit report recommendations	

Guidance attribute	Which MAPs guidance applies
Coast Guard Corrective Action Plan Desk Guide	Federal Financial Management Improvement Act of 1996 noncompliance–related control deficiency MAPs not related to material weaknesses or significant deficiencies.
1. Corrective action plan status	
2. Completion status	
3. Assigned to	
4. Original completion target date	
5. Updated completion target date	
6. Issue	
7. Requirement	
8. Root cause	
9. Action plan	
10. Related NFR	
11. Milestone number	
12. Milestone topic	
13. Green book principle	
14. Process owner	
15. Target completion	
16. Actual completion date	
17. Extension request date	
18. Completion status	

Legend: DHS = Department of Homeland Security; MAP = mission action plan; OMB = Office of Management and Budget; NFR = Notice of Findings and Recommendations.

Source: GAO analysis of OMB and DHS guidance. | GAO-23-105194

Appendix VI: Comments from the Department of Homeland Security

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

Homeland Security

February 9, 2023

Paula M. Rascona
Director, Financial Management and Assurance
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-23-105194, "DHS FINANCIAL MANAGEMENT: Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues"

Dear Ms. Rascona:

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

Senior DHS leadership is pleased to note GAO's positive recognition of the significant effort and resources DHS has devoted to challenges involving DHS's Financial Systems Modernization (FSM) program. GAO acknowledged progress made related to improving financial management functions and fully addressing two of the eight high-risk financial management actions and outcomes, partially addressing three others, and having initiated actions to address the remaining three. The report also noted ongoing system and data migration challenges at the U.S. Coast Guard, which we are working aggressively to address.

DHS has taken actions to establish a process to document and consider lessons learned to inform future modernization programs and efforts. DHS is committed to strengthening the FSM program, which focuses on achieving financial systems modernization throughout the Department. DHS will continue to apply sound program and risk management best practices to achieve its modernization goals.

The draft report contained four recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted

technical comments addressing several accuracy, contextual, and other issues under separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2023.02.09 10:13:48 -05'00'

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

Enclosure

2

Enclosure: Management Response to Recommendations Contained in GAO-23-105194

GAO recommended that DHS's Under Secretary for Management:

Recommendation 1: Ensure that the Joint Program Management Office [JPMO] works with Coast Guard to remediate known issues identified from testing, prior to declaring full operational capability for the ongoing financial systems modernization efforts.

Response: Concur. The FSM JPMO will work with the Trio[1] Components and DHS acquisition oversight offices to identify and agree upon what needs to be improved in the modernized system so that the Components can support a full operational capability (FOC) decision and the program can advance to an Acquisition Decision Event 3 (ADE-3).[2] This effort will likely require adjustments or clarification to approved Key Performance Parameters, requirements, and FOC definitions. Any changes to previously approved parameters will be made in the most transparent manner possible and will be subject to standard approval protocols, such as by the FSM/Trio Executive Steering Committee.

The FSM JPMO will develop and submit a breach remediation plan, which will include a/an:

a. Root cause analysis of the performance issues resulting in the inability to reach FOC;
b. Explanation of efforts that the JPMO will undertake to address performance, schedule, and cost issues;
c. Identification of actions that the JPMO will take to address the issues and recommendations that the Director of Operational Test and Evaluation identified in the System Evaluation Report;
d. Test and Evaluation Strategy to support declaration of FOC; and
e. Schedule to re-baseline the program to include an updated Life Cycle Cost Estimate and Acquisition Program Baseline.

Estimated Completion Date (ECD): March 31, 2023.

[1] The FSM Trio Program is the DHS Acquisition Program that modernized the financial management system of the U.S. Coast Guard, Transportation Security Administration, and the Countering Weapons of Mass Destruction Office.
[2] ADE-3 refers to deploying a system to the end user(s) and continuing to support and sustain it through its life cycle.

3

Recommendations 2: Ensure that the Joint Program Management Office works with FEMA [Federal Emergency Management Agency] to remediate issues as they arise from user testing prior to moving forward with subsequent milestones for the ongoing financial systems modernization efforts.

Response: Concur. The JPMO will ensure that lessons learned from the Trio implementation translate into appropriate actions for the ongoing FEMA financial systems modernization efforts, including comprehensive discovery efforts to develop functional requirements documentation, incorporating standard DHS business processes, and detailed user acceptance testing. Further, we will ensure alignment with generated requirements and complete the resolution of identified issues prior to go-live. Data quality concerns identified from prior lessons learned are being incorporated into planned data normalization efforts during the migration of data from legacy systems into FSM.

One critical lesson learned that will be incorporated in the FEMA (and ICE) modernization efforts is the need for early and consistent hands-on user testing throughout the implementation. Big Bang[3] user acceptance test during a waterfall deployment process may result in too many defects identified too close to cutover for prompt remediation. Development methodologies for FEMA will ensure incremental development followed by user testing and feedback throughout the implementation prior to System Integration Testing and final User Acceptance Testing. The JPMO is actively coordinating with FEMA to ensure the right SMEs are identified, prepared, and made available throughout the implementation process to assist with key design decisions and incremental testing events.

Additionally, the JPMO will work with FEMA to ensure that contingency plans are in place to ensure that system conversion does not impact the ability to make critical disaster-related payments timely. This includes ensuring that legacy systems are available to continue with operations and developing strategies for a mid-year cutover should outstanding issues prevent cutover at the beginning of a fiscal year.

Actions	Estimated Completion Date (ECD)
Discovery effort initiated with System Integrator and Component Stakeholders	October 1, 2023
Discovery effort complete, with Discovery Report capturing plans to conduct incremental development and early involvement of user community in testing and feedback	March 31, 2024

[3] A 'Big Bang' methodology involves performing the entirety of the work at once (in this case, user testing and acceptance) in contrast to incremental or phased-in approaches, which break the work into smaller, more manageable pieces.

4

Approval granted by Acquisition Decision Authority at Acquisition Decision Event 2A to execute implementation activities as documented in Systems Engineering Life Cycle Tailoring Plan, Test and Evaluation Master Plan, and Integrated Master Schedule	September 30, 2024

Overall ECD: September 30, 2024.

Recommendation 3: Ensure that the Joint Program Management Office works with ICE [U.S. Immigration and Customs Enforcement] to remediate issues as they arise from user testing prior to moving forward with subsequent milestones for the ongoing financial systems modernization efforts.

Response: Concur. The JPMO will ensure that lessons learned from the Trio implementation translate into appropriate actions for the ongoing ICE and ICE customer financial systems modernization efforts,[4] including comprehensive discovery efforts to develop functional requirements documentation, incorporating business processes, and detailed user acceptance testing. Further, we will ensure alignment with generated requirements and complete the resolution of identified issues prior to go-live. Data quality concerns identified from prior lessons learned are being incorporated into planned data normalization efforts during the migration of data from legacy systems into FSM.

One critical lesson learned that will be incorporated in the ICE modernization efforts is the need for early and consistent hands-on user testing throughout the implementation. 'Big Bang' user acceptance test during a waterfall deployment process may result in too many defects identified too close to cutover for prompt remediation. Development methodologies for ICE will ensure incremental development followed by user testing and feedback throughout the implementation prior to System Integration Testing and final User Acceptance Testing. The JPMO is actively coordinating with ICE and its customer components to ensure the right SMEs are identified, prepared, and made available throughout the implementation process to assist with key design decisions and incremental testing events.

Actions	ECD
Discovery effort initiated with System Integrator and Component Stakeholders	October 1, 2023
Discovery effort complete, with Discovery Report capturing plans to conduct incremental development and	March 31, 2024

[4] The FSM Cube Program is the DHS Acquisition Program with the goal of modernizing the financial management system of ICE and its Component customers: the Cybersecurity and Infrastructure Security Agency, DHS Headquarters Management, Science &Technology Directorate, and U.S. Citizenship and Immigration Services.

early involvement of user community in testing and feedback	
Approval granted by Acquisition Decision Authority at Acquisition Decision Event 2A to execute implementation activities as documented in Systems Engineering Life Cycle Tailoring Plan, Test and Evaluation Master Plan, and Integrated Master Schedule	September 30, 2024

Overall ECD: September 30, 2024.

Recommendation 4: Ensure that Coast Guard follows applicable guidance when developing corrective action plans to include documenting the root cause analysis and other recommended attributes.

Response: Concur. The Coast Guard Office of Financial Policy, Reporting, and Property (CG-84) follows applicable guidance, specifically using DHS' Mission Action Plan (MAP) Guidance and templates to build out and track corrective action plans for deficiencies identified during audits. Senior Assessment Team (governance) meetings are held monthly to manage this process with the Key Process Owners' (KPO) leadership. Additionally, the Coast Guard Comptroller leads briefs to the Vice Commandant at least quarterly at higher level governance meetings (Executive Management Council – Audit, Risk, and Compliance) so all levels across the organization are fully aware of this process.

Coordinating with the Coast Guard Office of Internal Controls (CG-85) and the Office of Cybersecurity Program Management (CG-62), CG-84 is currently developing 19 MAPs (for material weaknesses and significant deficiencies) and one Corrective Action Plan (for control deficiencies). The KPOs will propose remediation timelines that are vetted by Coast Guard leadership and then reviewed and approved by the DHS Risk Management and Assurance Office. ECD: May 31, 2023.

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

Paula M. Rascona, (202) 512-9816 or rasconap@gao.gov

Staff Acknowledgments

In addition to the contact named above, Michael LaForge (Assistant Director), Heather Rasmussen (Analyst-in-Charge), Veronica Cadiz-Rodriguez, Grace Gwin, Deanna Kitchens, Lisa Rowland, and Anne Thomas made key contributions to this report. Other contributors include Marcia Carlsen, Lauren S. Fassler, Patrick Frey, Jason Kelly, Shannin O'Neill, Anne Rhodes-Kline, and Kimberly Young.

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