Integrated Strategy for High-Risk Management

Strengthening Department of Homeland Security Management Functions

A Biannual Update to the Government Accountability Office

September 2022

Homeland Security

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

Homeland Security

October 11, 2022

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Comptroller General Dodaro:

On behalf of the Department of Homeland Security (DHS or the Department), I am pleased to submit the enclosed update to the DHS *Integrated Strategy for High-Risk Management* (*Integrated Strategy*).[1] In the transmittal for our March 2022 *Integrated Strategy* we asked that the Government Accountability Office (GAO) carefully consider removing *Strengthening DHS Management Functions* from the List when it issues the 2023 High-Risk Series report. From the Department's perspective, DHS operational outcomes, underpinned by effective management functions, demonstrate that the state of DHS management is strong and, most importantly, that the remaining challenges do not constitute a high-risk when viewed through the lens of the qualitative and quantitative factors GAO considers when designating a program high-risk.[2]

We appreciate GAO's positive engagement with the Department on our request, especially the DHS-wide leadership meetings held on April 19, 2022 and July 27, 2022, with the next scheduled for October 18, 2022. These and other meetings have provided an opportunity to demonstrate the actions DHS leaders have taken to institutionalize our commitment to addressing the *Strengthening DHS Management Functions* issue area and enable sustained success in the Department's endeavors, and to address any remaining GAO concerns about this work. Today, the challenges DHS faces in this area truly are minor in comparison to the conditions that led to GAO's original high-risk designation in 2003 and the subsequent 2013 high-risk update that narrowed the scope of that designation.

Through all the progress made to resolve high-risk issues, senior DHS leadership's focus has not let up, nor has the Department's commitment to maintaining a constructive partnership with GAO. For example, Secretary Mayorkas declared "GAO High-Risk" one of the top focus areas in a new Secretary's Infrastructure Transformation initiative announced at the beginning of

[1] The *Integrated Strategy*, published every six months since 2011, outlines the Department's framework for addressing the *Strengthening Department of Homeland Security Management Functions* (*Strengthening DHS Management Functions*) issue area on the Government Accountability Office (GAO) High-Risk List (the List).
[2] Reference GAO-21-119SP, "HIGH-RISK SERIES: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas," dated March 2, 2021, page 4 (PDF page 10).

fiscal year (FY) 2022. As part of this initiative, which is overseen by Deputy Secretary Tien, the Secretary directed leaders and program officials throughout DHS to redouble efforts to address our high-risk issues and related open high-risk and priority recommendations. As of September 14, 2022, the Department is on pace to close or have submitted to GAO for closure consideration by December 31, 2022, 98 percent (103 of 105) the recommendations identified in the initiative's original closure target.[3]

Admittedly, some challenging work remains. For example, financial management is a major component of the *Strengthening DHS Management Functions* high-risk area. In this area, DHS has continued to make progress modernizing outdated financial systems. The Department's highest modernization priority was the U.S. Coast Guard's (USCG) legacy system, which had cybersecurity weaknesses and lacked necessary business functionality, forcing USCG staff to perform key processes manually outside the system. In FY 2021, DHS moved the Transportation Security Administration, which shared USCG's system, to a modern platform. In FY 2022, DHS moved USCG itself to the same modern platform, allowing USCG to sunset its legacy system. Throughout FY 2022, the Acting Chief Financial Officer has assisted USCG as they worked to stabilize operations on the new system and generate positive audit outcomes. Finally in FY 2022, DHS commenced procurement activities to obtain modern systems for the Federal Emergency Management Agency and U.S. Immigration and Customs Enforcement. Those projects are on track for award in the first half of FY 2023.

DHS continues to believe the remaining risks in financial management or other functions related to *Strengthening DHS Management Functions* (i.e., acquisition management, information technology management, human capital management, and management integration) do not rise to the level of "high-risk," such that the functions are inherently vulnerable to fraud, waste, abuse, mismanagement, or need transformation beyond what one typically sees in government programs, operations, and activities. DHS strives to minimize risk; however, the Department recognizes that eliminating all risk is an aspirational goal—some degree of risk will always exist. DHS believes the salient question is "*how much risk is high-risk*," especially when considering the competing priorities and demands with increasingly constrained resources available to fulfill the Department's broad and complex mission in as effective a manner as possible, while upholding public trust and stewardship.

We renew our request that GAO carefully consider removing *Strengthening DHS Management Functions* from the List, and again thank GAO for the constructive relationship we have had working this issue since 2003.

Sincerely,

RANDOLPH D ALLES

Digitally signed by RANDOLPH D ALLES
Date: 2022.10.11 13:15:14 -04'00'

R.D. Alles
Acting Under Secretary for Management

[3] DHS continues to strictly adhere to a self-imposed practice of not closing any GAO recommendations without first reaching agreement with GAO staff to do so. This provides Congress and the public added confidence that appropriate actions were taken to implement these recommendations or otherwise resolve any disagreements.

Progress on GAO High-Risk Outcomes

This document provides corrective action plans for achieving the eight outcomes that have not yet achieved a Fully Addressed rating by GAO[1]. In 2010, GAO identified the outcomes and DHS agreed that achieving these goals is critical to addressing challenges within the Department's management areas and improving integration of management functions across DHS. The outcomes cover the functional areas of financial management, human capital, information technology, acquisition, and management integration. GAO rates the Department's progress on the outcomes using the following scale:

- **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.[2]

Subsequent to each *Integrated Strategy* update, GAO meets with DHS officials to provide feedback on progress, identify areas where additional work remains, and review outcome ratings. In recent years, DHS has steadily improved its progress as measured by the number of outcomes receiving a Fully Addressed or Mostly Addressed rating. For example, as of September 2022, GAO rated DHS as Fully Addressed or Mostly Addressed for 77% (23 of 30) of the outcomes, up from 70% in 2018 and 47% in 2015. *Table 1* provides a functional-level summary of 2020 GAO outcome ratings.

Table 1. Summary of GAO Outcome Ratings by Functional Area

Functional Area	Total GAO Outcomes	Fully Addressed	Mostly Addressed	Partially Addressed	Initiated
Financial Management	**8**	2	0	3	3
Human Capital Management	**7**	7	0	0	0
Information Technology Management	**6**	5	0	1	0
Acquisition Management	**5**	5	0	0	0
Management Integration	**4**	3	1	0	0
Total as of September 2022	**30**	**22**	**1**	**4**	**3**

The Department first issued the *Integrated Strategy* in 2011 and has maintained a practice of updating GAO twice yearly.[3] In general, the *Integrated Strategy* report provides updated action plans for the outcomes that have not yet achieved a Fully Addressed rating from GAO.

[1] GAO provided DHS officials with proposed 2023 outcome ratings in July 2022. Official ratings will be published in GAO's 2023 High-Risk List report.
[2] GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 3, 2021), page 180.
[3] Congress codified this practice by requiring DHS to report to GAO every six months. *National Defense Authorization Act for Fiscal Year 2017*, Public Law 114-328 § 1903(b) ((codified at 6 U.S.C. § 341(a)(11)), page 674.

Progress on GAO High-Risk Outcomes

Progress on GAO High-Risk Outcomes

Financial Management Outcomes #2 and 4

Outcome Lead: Alyssa Smiley

Outcome Executive: Stacy Marcott

GAO Outcomes: (FM 2) Obtain an unmodified opinion on internal control over financial reporting (ICOFR) to demonstrate effective internal controls; and (FM 4) Sustain unmodified opinions for at least two consecutive years on internal control over financial reporting (ICOFR).

DHS Successes: DHS has proven its capacity and capability for strong financial reporting and management, as noted by nine consecutive unmodified ("clean") financial statement opinions and the reduction of material weaknesses from ten in 2006 down to the remaining two. Specifically, in FY2020 DHS was able to fully remediate a long-standing significant deficiency over Property, Plant, and Equipment. Furthermore, the Department remediated the portion of the Financial Reporting material weakness associated with actuarial retirement liabilities – these liabilities totaled $67.3 billion at the end of FY 2020 – roughly half of total DHS liabilities. In FY 2021, DHS downgraded the Journal Voucher and Beginning Balance deficiency from being a contributor to the Financial Reporting material weakness. Given this demonstrated record of success, DHS does not believe that the current modified opinion on ICOFR poses a substantial, unmitigated risk to successful financial management at DHS.

GAO 2023 Outcome Rating: FM 2

Initiated	**Partially Addressed**	Mostly Addressed	Fully Addressed

GAO 2023 Outcome Rating: FM 4

Initiated	Partially Addressed	Mostly Addressed	Fully Addressed

CURRENT STATUS

To advance to Fully Addressed for Financial Management Outcome (FM) 2, DHS must obtain an unmodified opinion on internal control over financial reporting (ICOFR)and demonstrate an effective system of internal controls. To achieve an unmodified opinion, DHS must reduce one of the outstanding areas of material weakness to a significant deficiency. Once the unmodified opinion is obtained, DHS plans to use the same risk-based approach used for FM 2 to sustain the unmodified opinion and advance FM 4.

DHS continues to make significant progress and achieved its ninth unmodified audit opinion on the 2021 DHS financial statements and related footnotes. In addition, the sustainment of a "clean" financial statement opinion for nine years provides continued evidence that DHS has implemented the internal control over financial reporting sufficient to ensure that year-end financial reporting is not materially misstated. Given this demonstrated record of success, DHS does not believe that the current modified opinion on ICOFR poses a substantial, unmitigated risk to successful financial management at DHS.

With two remaining areas of material weakness in internal controls—in Financial Reporting and Information Technology—the Department's Chief Financial Officer (CFO) is executing a multi-year plan to achieve an unmodified "clean" ICOFR opinion by FY 2024. The Department recognizes remediation of the remaining areas of material weakness is the most challenging phase of the strategy to achieve a "clean" ICOFR opinion, due to the complexity resulting from DHS's many CFO-designated systems (with a combination of legacy systems as well as some in various stages of modernization), the need to rely on manual compensating controls in the interim, and the abundance of information and data utilized in DHS business process activities. The Department anticipates making substantial annual progress and continues to build upon its successful internal control enterprise approach, demonstrating incremental and sustainable progress each year, and remains collectively focused on the FY 2024 target.

OUTCOME ACTION PLAN[1]			
Actions	**Projected Date**	**Actual/Adjusted Date(s)**	**Reason for change/notes**
(FM 4) Sustain an unmodified (i.e., clean) opinion on internal control over financial reporting for two consecutive years (i.e., FY 2024 and FY 2025).	November 2025		**Targeting a Fully Addressed rating**. The independent auditor will issue its report for FY 2025 in November 2025.
(FM 4) Components re-evaluate risks to sustaining a clean audit opinion and reducing weaknesses in internal control and business processes.	March, June, and August 2025		Components identify risks that could prevent sustainment of progress and develop appropriate risk response.
(FM 4) DHS CFO to oversee and review A-123 results.	March, June, and August 2025		CFO incrementally reviews Component A-123 assessment results and sustains progress.
(FM 4) Demonstrate measurable progress by continuing to reduce weaknesses in internal control and business processes.	November 2024		**Targeting a Mostly Addressed Rating** The independent auditor will issue its report for FY 2024 in November 2024. This should be noted as "Mostly Addressed" when DHS Financial Management Outcome #2 is noted as "Fully Addressed". DHS proposes this Outcome be considered Mostly Addressed when all areas of material weakness have been reduced to a significant deficiency.
(FM 2) Obtain an unmodified (i.e., clean) opinion on internal control over financial reporting for FY 2024.	November 2024		**Targeting a Fully Addressed rating.** The independent auditor will issue its report for FY 2024 in November 2024. Adjusted date because select, complex deficiencies are taking longer to fix than originally anticipated. DHS proposes this outcome be considered Fully Addressed when no material weaknesses exist, and minimal significant deficiencies remain.
Components re-evaluate risks to sustaining a clean audit opinion and reducing weaknesses in internal control and business processes.	March, June, and August 2024		Components review the results of testing for the second and third quarters to continue to assess their progress as part of routine monitoring.

[1] Only the most recent and significant updates have been included in this report. For a history of the Department's progress in this area, please refer to past updates to the Integrated Strategy.

OUTCOME ACTION PLAN[1]			
Actions	**Projected Date**	**Actual/Adjusted Date(s)**	**Reason for change/notes**
DHS CFO to review and validate Component completed remediation steps.	March, June, and August 2024		DHS CFO incrementally reviews and validates remediation steps completed by Components.
DHS CFO will work with Components to assess FY 2023 audit risks and develop corrective actions.	January / February 2024		
(FM 4) Demonstrate measurable progress by continuing to reduce weaknesses in internal control and business processes.	November 2020	November 2023	**Targeting a Partially Addressed Rating** DHS proposes this Outcome be considered Partially Addressed when the Financial Reporting or IT material weakness area is reduced to a significant deficiency. This should be noted as "Partially Addressed" when DHS Financial Management Outcome #2 is noted as "Mostly Addressed". DHS has designed a repeatable process to address the audit conditions. Enhanced audit scope and deficiencies highlighted related to Information Produced by the Entity that will take additional time to remediate.
(FM 2) Demonstrate measurable progress by continuing to reduce weaknesses in internal control and business processes.	November 2023		**Targeting a Mostly Addressed rating.** The independent auditor will issue its report for FY 2023 in November 2023. DHS expects to downgrade one area of material weakness and clear one significant deficiency in FY 2023. DHS has designed a repeatable process to address the audit conditions and will be executing designed controls and testing to demonstrate effectiveness. DHS proposes this outcome be considered Mostly Addressed when the Financial Reporting or IT material weakness area is reduced to a significant deficiency.
Components re-evaluate risks to sustaining a clean audit opinion and reducing weaknesses in internal control and business processes.	March, June, and August 2022, 2023		Complete for 2022. Components review the results of testing for the second and third quarters to continue to assess their progress as part of routine monitoring.

OUTCOME ACTION PLAN[1]			
Actions	**Projected Date**	**Actual/Adjusted Date(s)**	**Reason for change/notes**
DHS CFO to review and validate Component completed remediation steps.	March, June, and August 2022, 2023		Complete for 2022. DHS CFO incrementally reviews and validates remediation steps completed by Components.
DHS CFO will work with Components to assess audit risks and develop corrective actions.	December 2021, January / February 2022, 2023		Complete for 2022. DHS CFO works with Components to establish corrective actions based on risks identified.

Financial Management Outcome #5

Outcome Lead: Alyssa Smiley

Outcome Executive: Stacy Marcott

GAO Outcome: 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.[1]

DHS Successes: DHS has proven its capacity and capability for strong financial reporting and management, as noted by nine consecutive unmodified ("clean") financial statement opinions and the reduction of material weaknesses from ten in 2006 down to the remaining two. While the FY 2021 independent auditor report noted areas of FFMIA noncompliance, DHS was no longer highlighted as noncompliant with the requirement for financial management systems to comply with the U.S. Standard General Ledger (USSGL) at the transaction level. Given this demonstrated record of success and dedicated commitment for additional remediation and control enhancements, DHS does not believe that the current modified opinion on Internal Control over Financial Reporting (ICOFR) and remaining challenges with FFMIA pose a substantial, unmitigated risk to successful financial management at DHS.

GAO 2023 Outcome Rating

Initiated	**Partially Addressed**	Mostly Addressed	Fully Addressed

CURRENT STATUS

FFMIA Section 803(a) requires that agency Federal financial management systems comply with (1) applicable Federal accounting standards; (2) Federal financial management system requirements; and (3) the USSGL at the transaction level. DHS monitors and assesses Component financial systems for compliance with FFMIA Section 803(a) requirements for its core financial management systems. In addressing compliance, DHS follows the Office of Management and Budget (OMB) Compliance Framework.[2] The DHS Chief Financial Officer (CFO) ensures procedures are in place to provide guidance that summary adjustments posted in the financial system(s) are traceable to the transaction source, and ensures Components accurately report instances of non-conformance to generally accepted accounting principles.

To further strengthen management, DHS, through a CFO/Chief Information Officer (CIO) integrated approach and strategy, is conducting the following activities:

- Requiring Components to document necessary actions to remediate information technology (IT) security control weaknesses in their corrective action plans. The Department's independent auditor reviews Component compliance with FFMIA annually.
- Continuing remediation efforts to downgrade the Financial Reporting weakness area to a significant deficiency by FY 2022 and reducing the severity of the IT weakness area to a significant deficiency by FY 2024 in order to meet OMB Circular A-123 Appendix D requirement for complying with FFMIA.
- Assessing the Department's FFMIA compliance utilizing the compliance framework as outlined in OMB Circular A-123. DHS plans to be FFMIA-compliant by FY 2024, as the Department expects to remediate the IT and Financial Reporting areas of material weakness by then, as well as achieve compliance with the Federal Information Security Modernization Act of 2014.

For FY 2022, Components have submitted commitment letters to the DHS leadership highlighting each Component's plan and timeline to perform / submit assessment and remediation deliverables in support of the ICOFR business processes as well as for the CFO Designated Systems. Remediation and assessment efforts are ongoing in support of the Department's find, fix, test, and assert strategy.

[1] *Federal Financial Management Improvement Act (FFMIA)*, Congress Public Law No. 104-208, 104th, September 30, 1996.
[2] Office of Management and Budget, *Management's Responsibility for Internal Control, OMB Circular A-123* (Washington, D.C.: September 20, 2013), *Appendix D, Compliance with the Federal Financial Management Improvement Act of 1996.*

OUTCOME ACTION PLAN[3]			
Actions	**Projected Date**	**Actual/Adjusted Date(s)**	**Reason for change/notes**
Substantially comply with the requirements of FFMIA as reported by the independent auditor.	November 2024		**Targeting a Fully Addressed rating.** The independent auditor will issue its report for FY 2024 in November 2024. The Department proposes this outcome be considered Fully Addressed when DHS downgrades the material weaknesses in Financial Reporting and in IT, to satisfy the FFMIA requirement regarding Federal financial management system requirements, based on OMB's updates to Circular A-123.
Components re-evaluate risks to sustain a clean audit opinion and reduce weaknesses in internal control and business processes.	March, June, and August 2024		Components review the results of testing for the second and third quarters to continue to assess their progress as part of routine monitoring.
Conduct quarterly risk assessments and incorporate results into Component risk management plans through recurring quarterly meetings.	December 2023; April and July 2024		Risk assessment meetings track progress being made on areas needing most improvement, or areas that would significantly impact ability to reduce weaknesses in internal control and business processes.
DHS CFO to engage with Component CFOs to review the status of addressing audit findings, risks, and mitigation strategies.	December 2023 through August 2024		Monthly action.
The Independent Auditor's Report notes further improvement in Component FFMIA compliance and indicates a reduction in the number of Components contributing to the IT and Financial Reporting conditions.	November 2023		**Targeting a Mostly Addressed Rating.** The independent auditor will issue its report for FY 2023 in November 2023. DHS proposes this Outcome be considered Mostly Addressed when the Financial Reporting or IT material weakness area is reduced to a significant deficiency. Based on the DHS strategy and Component plans to resolve existing deficiencies, DHS is targeting to reduce the Financial Reporting area of material weakness in FY 2023.

[3] Only the most recent and significant updates have been included in this report. For a history of the Department's progress in this area, please refer to past updates to the Integrated Strategy.

OUTCOME ACTION PLAN[3]			
Actions	**Projected Date**	**Actual/Adjusted Date(s)**	**Reason for change/notes**
Components re-evaluate risks to sustain a clean audit opinion and reduce weaknesses in internal control and business processes.	March, June, and August 2023		Components review the results of testing for the second and third quarters to continue to assess their progress as part of routine monitoring.
Conduct quarterly risk assessments and incorporate results into Component risk management plans through recurring quarterly meetings.	December 2022; April and July 2023		Risk assessment meetings track progress being made on areas needing most improvement, or areas that would significantly impact ability to reduce weaknesses in internal control and business processes.
DHS CFO to engage with Component CFOs to review the status of addressing audit findings, risks, and mitigation strategies.	December 2022 through August 2023		Monthly action conducted each year (completed for FY 2022).
Components re-evaluate risks to sustain a clean audit opinion and reduce weaknesses in internal control and business processes.	March, June, and August 2022		Partially Complete. Components review the results of testing for the second and third quarters to continue to assess their progress as part of routine monitoring (conducted each year).
Conduct quarterly risk assessments and incorporate results into Component risk management plans through recurring quarterly meetings.	December 2021; April and July 2022		Completed (conducted each year).
The Independent Auditor's Report notes further improvement in Component FFMIA compliance and indicates a reduction in the number of Components contributing to the IT and Financial Reporting conditions.	November 2016	November 2020	Completed. While DHS had planned to clear the Financial Reporting material weakness in the FY 2020 audit report, both the Financial Reporting and Information Technology material weaknesses remain. However, DHS was able to clear the Property, Plant, and Equipment significant deficiency and removed a Component from contributing to the IT area of material weakness.

Financial Management Outcomes #6–8

Outcome Lead: Jeffrey Bobich

Outcome Executive: Stacy Marcott

GAO Outcome: Effectively manage the implementation of a financial management system solution or modernization of existing systems for the U.S. Coast Guard (USCG) and its customers; Federal Emergency Management Agency (FEMA); and U.S. Immigration and Customs Enforcement (ICE) and its customers by:

- Applying rigorous and disciplined information technology (IT) acquisition management processes throughout the program/project lifecycle that is consistent with software engineering best practices. These steps will help to ensure that the systems meet expected capabilities/requirements and associated mission benefits.
- Implementing oversight mechanisms to monitor contractors or shared service providers selected to implement the solution or modernize the existing systems. These steps will help to ensure that actual cost, schedule, and performance are within established threshold baselines, and variances are identified, tracked, and addressed.

DHS Successes: DHS successfully completed modernization for the first "Trio" of Components – Countering Weapons of Mass Destruction Office (CWMD), Transportation Security Administration (TSA), and USCG – using a rigorous and disciplined acquisition management process with strong oversight and monitoring of contractors. DHS has sustained an unmodified financial statement audit opinion for nine consecutive years – including the years immediately after the CWMD and TSA modernizations. Given this demonstrated record of success, we will continue to be successful with FEMA and ICE modernization. While challenging, these programs are not a risk to successful financial management at DHS – FEMA and ICE have been able to produce accurate, auditable financial data despite their outdated systems.

GAO 2023 Outcome Rating: FM 6 (USCG)

Initiated	**Partially Addressed**	Mostly Addressed	Fully Addressed

GAO 2023 Outcome Rating: FM 7 (FEMA) and 8 (ICE and ICE Customers)

Initiated	Partially Addressed	Mostly Addressed	Fully Addressed

CURRENT STATUS

DHS consolidated action plans for financial systems modernization (FSM) efforts into a single plan that reflects the Department's consolidated strategy and program management approach.

The system integrator delivered all TSA functionality in FY 2020, and TSA went live on the solution in Q1 FY 2021. In Q3 FY 2021, the solution was moved to a cloud environment. USCG successfully transitioned to the solution in Q1 FY 2022. In December 2021, DHS provided GAO notice of USCG's completed transition to the new financial system and requested GAO update the status of FM 6 to "Fully Addressed." In July 2022, GAO stated that they are waiting on the FY 2022 USCG audit report and results from the full operating capability assessment before making a decision on whether to change the status of this outcome.

FEMA (FM 7) and ICE and ICE Customers (FM 8):

- The procurement process to select software and integration service providers for FEMA and ICE is currently in progress. DHS anticipates award of software task orders by the end of October 2022, and integration task orders by the end of January 2023. Following those awards, DHS will conduct a discovery process with the software vendors and integrators. Implementation plans, with key milestone dates, will be an output from that process.

OUTCOME ACTION PLAN[1]			
Actions	**Projected Date**	**Actual/Adjusted Date(s)**	**Reason for change/notes**
FM 6			
USCG completes migration of their financial management systems.	October 2021	December 2021	**Completed:** USCG migration is complete, and GAO Outcome FM 6 is complete.[2]
USCG go live.	October 2021	December 2021	Completed. USCG went live Dec. 17, 2021.
TSA completes migration of their financial management systems.	October 2020	October 2020	**TSA migration is complete.**
TSA go live.	October 2020	October 2020	TSA went live on 30 October 2020.
FM 7			
FEMA completes migration of their financial management systems.	TBD		**Targeting a Fully Addressed rating for GAO Outcome FM 7.**
FEMA go live.	TBD		Component will present documentation to support that the solution is ready for deployment and support.
FEMA Program status review.	TBD		End users will receive new system and business process training.
FEMA Data conversion and migration.	TBD		End users will test and accept system software based on their requirements and approved test plans.
FEMA Training.	TBD		Data will be incorporated from old to new system.
FEMA Test and acceptance.	TBD		System provider will configure system software to meet requirements.
DHS completes configuration and interfaces for FEMA.	TBD		
Discovery phase.	TBD		
Select the system integrator.	January 2023		Changes to procurement schedules.
Select the software.	October 2022		Changes to procurement schedules.

[1] Only the most recent and significant updates have been included in this report. For a history of the Department's progress in this area, please refer to past updates to the Integrated Strategy.

[2] In July 2022, GAO stated that they are waiting on the FY 2022 USCG audit report and results from the full operating capability assessment before making a decision on whether to change the status of this outcome.

OUTCOME ACTION PLAN[1]			
Actions	**Projected Date**	**Actual/Adjusted Date(s)**	**Reason for change/notes**
Strategic Sourcing Software Licensing vehicle.	TBD	February 2022	Enterprise Financial Management Software (EFIMS) was awarded in September 2021. A protest was resolved in February 2022.
Strategic Sourcing System Integration (SI) vehicle.	Q2 FY 2020	March 2021	Completed. Enterprise Financial Systems Integrator (EFSI) vehicle was awarded November 2020, and protest resolved favorably in March 2021.
FM 8			
ICE and other ICE Customers (i.e., CISA, S&T, and DMO) complete migration of their financial management systems.	TBD		**Targeting a Fully Addressed rating for GAO Outcome FM 8.**
ICE and other ICE Customers go live.	TBD		Component will present documentation to support that the solution is ready for deployment and support.
ICE and other ICE Customers Program status review.	TBD		End users will receive new system and business process training.
ICE and other ICE Customers Data conversion and migration.	TBD		End users will test and accept system software based on their requirements and approved test plans.
ICE and other ICE Customers Training.	TBD		Data will be incorporated from old to new system.
ICE and other ICE Customers Test and acceptance.	TBD		System provider will configure system software to meet requirements.
DHS completes configuration and interfaces for ICE and other ICE Customers.	TBD		
USCIS complete migration of their financial management systems.	TBD		**Targeting a Partially Addressed rating for GAO Outcome FM 8.** USCIS will be the first ICE Customer to pilot the financial management system. The Fully Addressed rating for GAO Outcome FM 8 will occur once ICE and other ICE Customers (i.e., CISA, S&T, and DMO) migrate to the financial management system.
USCIS go live.	TBD		Component will present documentation to support that the

OUTCOME ACTION PLAN[1]			
Actions	**Projected Date**	**Actual/Adjusted Date(s)**	**Reason for change/notes**
			solution is ready for deployment and support.
USCIS Program status review.	TBD		End users will receive new system and business process training.
USCIS Data conversion and migration.	TBD		End users will test and accept system software based on their requirements and approved test plans.
USCIS Training.	TBD		Data will be incorporated from old to new system.
USCIS Test and acceptance.	TBD		System provider will configure system software to meet requirements.
DHS completes configuration and interfaces for USCIS.	TBD		
Discovery phase.	TBD		
Select the system integrator.	January 2023		Changes to procurement schedules.
Select the software.	October 2022		Changes to procurement schedules.
Strategic Sourcing Software Licensing vehicle.	TBD	February 2022	Enterprise Financial Management Software (EFIMS) was awarded in September 2021. A protest was resolved in February 2022.
Strategic Sourcing System Integration (SI) vehicle.	Q2 FY 2020	March 2021	Completed. Enterprise Financial Systems Integrator (EFSI) vehicle was awarded November 2020, and protest resolved favorably in March 2021.

IT Management Outcome #6

Outcome Leads: Kenneth Bible/Luis Coronado

Outcome Executive: Eric Hysen

GAO Outcome: Enhance Information Technology (IT) Security – Establish enhanced security of the Department's internal IT systems and networks as evidenced by:

- Demonstrating measurable progress in achieving effective information system controls by downgrading the Department's material weakness in financial systems security to a significant deficiency for two consecutive years and reducing the deficiencies that contribute to the significant deficiency, as reported by the independent auditors of the Department's financial statements;
- Implement the federal desktop core configuration on applicable devices and instances across Components, as determined by an independent assessment;
- Promptly develop remedial action plans and demonstrate sustained progress mitigating known vulnerabilities, based on risk, as determined by an independent assessment; and
- Implement key security controls and activities, as independently assessed by the Office of Inspector General or external auditor based on *Federal Information Security Management Act of 2002* (FISMA) reporting requirements.

DHS Successes: DHS OCIO has fully addressed five of the six outcomes for Information Technology and has made progress toward resolution of the final outcome. At the same time, OCIO has rapidly deployed a series of technical solutions to meet emerging priorities across the Department, as well as steadily introducing key programs to integrate functions across the enterprise. One example is the Unified Cybersecurity Maturity Model (UCMM). DHS has implemented a UCMM framework to align cybersecurity spending and new cybersecurity capability requests to critical cybersecurity domains and current initiatives, further improving alignment between DHS and National Security Strategies. The UCMM framework has been a key in aligning recovery actions from the SolarWinds Incident and guiding implementation of critical cybersecurity capabilities and above guidance requests. Going forward, the framework provides a means to guide cybersecurity maturity level measurement for the Department.

The Department believes that it has largely addressed the issues and concerns raised in IT Management Outcome #6. DHS will separately present a rationale and supporting evidence to GAO for the removal of the high-risk designation on DHS IT Management, which includes monitoring the Department's activities consistent with other agencies in the context of the broader, government-wide "Ensuring the Cybersecurity of the Nation" GAO High-Risk area. Notwithstanding the Department's position, the action plan herein details the actions and milestones that GAO previously assessed as being necessary for ITM #6 to achieve a Fully Addressed rating.

GAO 2023 Outcome Rating

Initiated	**Partially Addressed**	Mostly Addressed	Fully Addressed

CURRENT STATUS

As previously agreed to with GAO, in order to reach Fully Addressed, DHS must achieve and sustain a downgrade of its material weakness in financial systems security to a significant deficiency for two consecutive years. The Department has implemented continuous monitoring of progress against the remediation work plan, identifying critical milestones, addressing audit risks, and reviewing mitigation strategies.

Internal Controls:

In a joint effort by the DHS CIO and the Chief Financial Officer (CFO), DHS has expanded the IT internal control program to assist in the monitoring and management of the IT internal controls for the Department

CURRENT STATUS

and jointly support Components in efforts to strengthen IT general controls, systems security, and IT internal controls environments.

DHS CISO has expanded the Independent Verification and Validation (IV&V) capabilities of Component IT to address Notices of Findings and Recommendations (NFR) remediation. This capability allows DHS CISO to verify the component and system personnel have remediated the finding appropriately as identified by the annual DHS Financial Statement Audit.

Key recommendations from various audits and assessments are incorporated in the FY Information Security Performance Plan (ISPP) and monitored for successful implementation across the Department through the monthly DHS FISMA Scorecard. DHS CISO Compliance staff meet on a regular basis with Component CISO staff to address the FISMA Scorecard deficiencies.

DHS has enhanced the Plan of Action and Milestones (POA&M) monitoring program to ensure the completeness and quality of remediation activity and POA&M management. The program consists of two reviews, a Weakness Remediation Completeness Review and POA&M Quality Review, which are described below. Both reviews are based on remediation completion evidence and POA&M data maintained in the Information Assurance Compliance System (IACS), reflected on the FISMA Weakness Remediation Scorecard.

DHS has developed remedial action plans and demonstrated sustained progress mitigating known vulnerabilities, based on risk, as determined by an independent assessment as noted throughout this document. Specifically, we have expanded our Independent Verification and Validation process, implemented a Unified Cybersecurity Maturity Model framework, established the Cybersecurity Service Provider Program (CSP), and established the Hack DHS Vulnerability Assessment Program.

DHS CIO continues to hold Component IT remediation status meetings prioritizing the weaknesses with the greatest impact to the Department with appropriate Component executives. For example, meetings are held routinely with Federal Emergency Management Agency (FEMA) and U.S. Coast Guard (USCG), who have the most complex remediation challenges. As a result of these meetings, approximately 50% of FY 2020 IT NFRs have been resolved.

Continuous Monitoring:

The DHS Cybersecurity Continuous Diagnostics and Mitigation (CDM) Program within DHS has been instrumental in effectively protecting Departmental network infrastructure by providing all DHS Components with the ability to leverage best-in-breed technologies that identify cybersecurity risks, develop mitigation strategies, and implement mitigations based on the potential impacts on all the DHS Component missions. Participating Components are reporting hardware asset management (HWAM), configuration settings management (CSM), and vulnerabilities (VULN) data to the Department's CDM Dashboard and generating cybersecurity risk scores. The DHS CIO is using CDM data to produce monthly risk dashboards and FISMA reports.

DHS has also finished implementation of Phase III Incident Response Reporting (IRR) capability within U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement Amazon Web Services (AWS) Gov Cloud environments and provided the Department with a central code repository to maintain and share cybersecurity playbooks across DHS, as well as, successfully trained thirty-three (33) Cybersecurity Analysts as Swimlane Certified Security Orchestration, Automation and Response (SOAR) Administrators/Developers for DHS.

Supply Chain Risk Management (SCRM):

The Department has accelerated its information communications technology (ICT) SCRM implementation, to include:

- Establishing programmatic and process discipline to manage information flows between intelligence, procurement, and other SCRM stakeholders.
- Developing Cyber Hygiene contract language, standards, and guidance that leverage lessons learned from both assessments of the cybersecurity posture of existing DHS vendors and the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) framework to ensure vendors handling DHS data or building DHS systems have mature cybersecurity programs to appropriately protect DHS data.

CURRENT STATUS

- Exploring the means by which to evaluate vendors with a focus not only upon self-declaration, but through independent assessment to verify sound cybersecurity processes are in use throughout their Software Development Life Cycle --particularly for commercial-off-the-shelf (COTS) products.
- Developing the means to continuously assess the range of products (software/hardware) and, services across the Enterprise to understand where corporate changes (mergers, buy-outs, offshoring, foreign interests, etc.) may pose risks to the integrity of products in the environment.

Furthermore, to accelerate vendor evaluation efforts following recent events, the DHS CIO is developing a vendor evaluation framework (based on contract complexity) by combining critical cybersecurity standards and best practices, and mapping controls and processes across several maturity levels that range from basic Cyber Hygiene to advanced. In close collaboration with the Office of the Chief Procurement Officer (OCPO) and Office of General Counsel (OGC), the DHS CIO had successfully completed an initial pathfinder assessment on an existing small business contract that contains DHS's Cyber Hygiene clauses and continues to further evaluate additional vendors. Through the complete implementation of this model:

- DHS will gain the vendor assurances/certifications needed to safeguard sensitive information across the DHS supply chain
- Remain the leader for government and industry driving good cyber hygiene practices that protect data and processes.

Cybersecurity:

The DHS Secretary has outlined a bold vision and implemented a roadmap for the Department's cybersecurity efforts to confront the growing threat of cyber-attacks, to drive action in the coming year, and to raise public awareness about key cybersecurity priorities. Across the enterprise, the Department's cybersecurity and critical infrastructure responsibilities focus on four key areas, including: securing federal civilian networks, strengthen the security and resilience of critical infrastructure, assessing and countering evolving cyber risks, and combatting cybercrime.

The DHS CIO has prioritized the collaboration with all Components to focus on successful implementation of key cybersecurity initiatives such as Cloud Modernization, implementing a Zero Trust Architecture through the incremental implementation of Zero Trust capabilities, accelerating capability delivery of the DHS Supply Chain Risk Management (SCRM) program, enhancing the DHS Cybersecurity Service Provider (CSP) program to provide cybersecurity maturity assessments to other federal agencies, and hardening Identity and Credential Access Management (ICAM) capabilities within the Department.

DHS CIO is also expanding the newly established 'Hack DHS' bug bounty program that leverages highly vetted and talented white hat hackers to search for vulnerabilities and weaknesses that are not detected in or detectable by day-to-day operations performed by DHS stakeholders.

DHS CFO and DHS CIO have prioritized the integration of cybersecurity risk into the DHS Enterprise Risk Management (ERM) framework to ensure Cybersecurity Risk is incorporated into the DHS-wide ERM process. The DHS CISO has formalized the DHS CISO Council which is the overarching governing body responsible for implementing a security program that meets DHS mission requirements, ensuring information security is a shared responsibility throughout DHS, and promoting a culture of Cybersecurity awareness. The Council meets monthly to discuss and coordinate the development of solutions across the Department.

In response to the SolarWinds supply chain attack in FY 21, DHS CIO has developed and approved a set of tailored network architecture and cybersecurity improvements to strengthen the DHS Enterprise network against future cyber-attacks. These improvements encompass maturity actions that restore confidence in the network, ensure continued mission success, and build a resilient DHS Enterprise network. Existing funding and resources have been aligned, or in some cases requested, to support the discrete actions to reduce the Department's susceptibility to cyber-attack.

- DHS has awarded four Enterprise Infrastructure Solutions (EIS) task orders for modernizing its telecommunications infrastructure with Internet Protocol-based networking services. Software defined wide area network (SD-WAN) and other cybersecurity protections will reduce the Department's attack surface by reducing discrete connections to the internet. This permits improved monitoring, in keeping with the ZT security model, which has become an increased focus in the aftermath of high-profile incidents like SolarWinds.

CURRENT STATUS

DHS is dedicating significant energy toward exceeding our cybersecurity hiring goal by recruiting talented experts, investing in diverse talent pipelines, and ensuring equitable access to professional development opportunities at every level. DHS has hired approximately 300 new cybersecurity professionals as part of a 60-day cyber workforce sprint launched in May 2021, and 500 more have tentative job offers.

OCIO in collaboration with the Office of the Chief Human Capital Officer (OCHCO) assisted in the development of a Cyber Talent Management System (CTMS). CTMS is a new mission-driven, person-focused, market-sensitive approach to hiring, compensating, and developing cybersecurity talent across DHS. CTMS has opened new options and strategies for staffing critical cybersecurity work, providing DHS Components with straightforward, agile operational processes with a focus on talent quality and maintaining cybersecurity mission readiness. With the launch of CTMS, DHS organizations, starting with CISA and OCIO, have begun using CTMS to hire, compensate, and develop DHS Cybersecurity Service employees. In addition, DHS has successfully implemented the Strategic Workforce Planning Initiative. This Initiative assessed the IT skills of HQ OCIO employees according to IT roles and identified training opportunities, gaps, and future needs.

DHS Cybersecurity Services Provider Program (CSP) has allowed DHS to assess the effectiveness and efficiency of Security Operation Centers (SOCs) and Network Operation Centers (NOCs) based on a standard framework of best practices. The establishment of DHS's CSP program has been a resounding success. Transition to this new model of cybersecurity service delivery has matured DHS's cybersecurity capabilities and promises to have a continued positive impact not only for DHS, but across the breadth of the Federal Government.

With a framework in place, the DHS CIO conducted a formal assessment of each DHS Component SOC in FY20, resulting in a subscriber-provider model that ensures all DHS endpoints get efficient and (more importantly) uniform protections against cyber adversaries. Since then, the DHS CIO, in Partnership with the Cyber Infrastructure Security Agency (CISA), has successfully conducted a formal assessment of the Department of Justice (DOJ) SOC, and has expanded assessments to include DHS Component NOC evaluations.

Network Operations Security Center (NOSC) Alignment:

DHS has consolidated the security and network operations functions under the NOSC. The DHS NOSC model helps DHS mitigate current cybersecurity challenges by providing simultaneous real-time operational and security situational awareness. This model also helps DHS to modernize, identify potential issues to prevent outages, and defend DHS assets from hostile threats. Lastly, it increases collaboration and integration in our network to:

- Remove visibility gaps;
- Increase tool automation;
- Integrate workflow and data feeds;
- Establish a follow the sun operational model to reduce seams in operational center visibility; and
- Provide redundancy.

SecDevOps:

To fully adopt agile software development, DHS is focused on making SecDevOps a standard practice to reduce costs while increasing security and stability across DHS. The SecDevOps methodology aims to alter culture and practice to create a delivery workflow that meets the needs of security, development, and operations stakeholders with minimal overhead. The DHS SecDevOps initiative includes security-focused automation, a reliable release pipeline, automation of common tasks, and solutions to enable stronger collaboration across all stakeholders (security, development, and operations), with the goal of deploying working functionality to the end-user faster.

The Federal Desktop Core Configuration:

DHS transitioned to the Defense Information Systems Agency (DISA) The Federal Desktop Core Configuration (FDCC) Secure Technical Implementation Guides for standardized configuration. FDCC was a standard for security-reliable Microsoft (MS) Windows operating system (Windows XP and Vista) running on desktop and laptop computers that were mandatory in 2008. The FDCC evolved into the U.S. Government Configuration Baseline (USGCB) which extended the original by including settings for Windows 7 and Red Hat Enterprise Linux 5 (RHEL 5). DHS moved to a more secure Operating System (OS) and configuration in 2018, when the

CURRENT STATUS
Chief Information Officer (CIO) directed adoption of Windows 10 Secure Host Baseline. As neither the FDCC nor the USGCB were applicable to Win10, in 2019, the DHS Chief Information Security Officer (CISO) directed Components to follow the Defense Information Systems Agency (DISA).

OUTCOME ACTION PLAN[1]			
Actions	**Projected Date**	**Actual/Adjusted Date(s)**	**Reason for change/notes**
Achieve and sustain "significant deficiency" status or less for two consecutive years (i.e., FY 2024 and 2025).	November 2021	November 2025	**Targeting a Fully Addressed rating.** The independent auditor will issue its report for FY 2025 in November 2025. Adjusted date because IT deficiencies are taking longer to fix than originally anticipated.
Complete actions to address five (5) recommendations contained in the OIG FY 2019 FISMA report (OIG-20-77).	Q1 FY 2022	September 2021	Completed. Recommendations 1, 3, and 5 are open and resolved, recommendation 2 is unresolved and open, and recommendation 4 is resolved and closed.

[1] Only the most recent and significant updates have been included in this report. For a history of the Department's progress in this area, please refer to past updates to the Integrated Strategy.

Management Integration Outcome #1

Outcome Lead: Ann-Marie Watt

Outcome Executive: Janene Corrado

GAO Outcome: Management Integration Implementation – Implement the actions and outcomes specified within each management area (acquisition, information technology, financial, and human capital management) to develop consistent or consolidated processes and systems within and across its management functional areas.

DHS Successes: Management functions provide support across the Department every day that enables successful DHS-wide mission performance. In January 2022, DHS leadership moved from half-yearly to quarterly meetings with GAO to provide regular updates on the Department's work to address High Risk Areas. During the January meeting, DHS emphasized its continued commitment to working productively, transparently, and collectively to improve DHS, as demonstrated with the inclusion of the GAO High-Risk List as one of the top priorities listed in the Secretary's Infrastructure Transformation (SIT) initiative. The SIT provides integrated Department-wide focus toward continued, substantial progress so that the only items remaining to be done are by their nature truly high-risk items.

GAO 2023 Outcome Rating

Initiated	Partially Addressed	**Mostly Addressed**	Fully Addressed

CURRENT STATUS

Per GAO, this Outcome will move to Mostly Addressed in the 2023 update to the High-Risk List report. This is a direct result of the significant progress made in the other functional areas.

The Department will advance the rating for this outcome by continuing to demonstrate sustainable progress integrating management functions within and across the Department, as well as continuing efforts to address the remaining outcomes that have yet to achieve a Fully Addressed rating.

- As of July 2022, GAO rated 77% (23 of 30) of outcomes as either Fully Addressed or Mostly Addressed[1] (including achieving Fully Addressed for all outcomes in acquisition and human capital). The Department's progress continues to build on its progress and has experience significant improvement compared to 47% (14 of 30) in 2015 and in 26% (8 of 31) in 2013.[2] Since the 2021 alone, DHS has advanced four outcomes to Fully Addressed.
- In July 2022, GAO notified DHS that the remaining acquisition program management outcomes will advance from Mostly Addressed to Fully Addressed in the 2023 update to the High-Risk List report.
- As of September 2022, *Strengthening Department of Homeland Security Management Functions* is one of only two remaining High-Risk areas to have met the majority of GAO's criteria for removal from the High-Risk List.[3]

[1] GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 3, 2021).
[2] GAO reduced the total number of outcomes from 31 to 30 in March 2014, between the 2013 and 2015 *High-Risk Series* reports.
[3] GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 3, 2021), page 19. In 2021, DOD Support Infrastructure Management met all five criteria and was removed from the list. In addition, segments of three other areas improved sufficiently that GAO removed these segments from the list.

OUTCOME ACTION PLAN[4]			
Actions	**Projected Date**	**Actual/Adjusted Date(s)**	**Reason for change/notes**
Engage GAO on the status of this Outcome upon transmission of the September 2023 *Integrated Strategy*.	December 2023		**Targeting a Fully Addressed rating.** GAO reported that for DHS to achieve this Outcome, the Department needs to continue demonstrating sustainable progress in addressing the remaining outcomes that have yet to achieve a Fully Addressed rating.[5]
Engage GAO on the status of this Outcome upon transmission of the March 2022 *Integrated Strategy*.	September 2022	July 2022	**Targeting a Mostly Addressed rating.** DHS will continue to demonstrate significant and sustainable progress on the remaining outcomes to achieve a Fully Addressed rating.
Continue to monitor GAO outcomes and publish the biannual *Integrated Strategy*.	March and September 2022	March and September 2022	DHS publishes the report twice a year.

[4] Only the most recent and significant updates have been included in this report. For a history of the Department's progress in this area, please refer to past updates to the Integrated Strategy.

[5] GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 2021), page 183.

GAO High-Risk Ratings Summary

GAO High-Risk Ratings Summary

Functional Area	GAO Outcome	2021 GAO Ratings[1]	2023 GAO Ratings[2]
FM 1	Clean opinion on all financial statements	Fully Addressed	Fully Addressed
FM 2	Clean opinion on internal controls	Partially Addressed	Partially Addressed
FM 3	Clean opinions for two years	Fully Addressed	Fully Addressed
FM 4	Clean opinions for two years on internal controls	Initiated	Initiated
FM 5	Compliance with FFMIA	Partially Addressed	Partially Addressed
FM 6	USCG Financial Systems Modernization	Partially Addressed	Partially Addressed
FM 7	FEMA Financial Systems Modernization	Initiated	Initiated
FM 8	ICE Financial Systems Modernization	Initiated	Initiated
HCM 1	Implement Human Capital Plan	Fully Addressed	Fully Addressed
HCM 2	Link workforce planning to other Department planning efforts	Fully Addressed	Fully Addressed
HCM 3	Enhance recruiting to meet current and long-term needs	Fully Addressed	Fully Addressed
HCM 4	Base human capital decisions on competencies and performance	Fully Addressed	Fully Addressed
HCM 5	Seek employee input to strengthen human capital approaches	Fully Addressed	Fully Addressed
HCM 6	Improve Federal Employee Viewpoint Survey Scores	Fully Addressed	Fully Addressed
HCM 7	Assess and improve training, education & development programs	Mostly Addressed	Fully Addressed
ITM 1	Achieve EAMFF Stage 4	Fully Addressed	Fully Addressed
ITM 2	Achieve ITIMF Stage 3	Fully Addressed	Fully Addressed
ITM 3	Achieve CMMI Level 2	Fully Addressed	Fully Addressed
ITM 4	Implement IT Human Capital Plan	Fully Addressed	Fully Addressed
ITM 5	Adhere to IT Program Baselines	Fully Addressed	Fully Addressed
ITM 6	Enhance IT Security	Mostly Addressed	Partially Addressed
APM 1	Timely validate required acquisition documents	Fully Addressed	Fully Addressed
APM 2	Improve Component acquisition capabilities	Fully Addressed	Fully Addressed
APM 3	Establish and effectively operate the Joint Requirements Council	Mostly Addressed	Fully Addressed
APM 4	Assess acquisition program staffing	Mostly Addressed	Fully Addressed
APM 5	Establish oversight mechanisms to validate that acquisition programs are achieving goals and comply with Department policies	Mostly Addressed	Fully Addressed
MI 1	Implement actions / outcomes in each LOB	Partially Addressed	Mostly Addressed
MI 2	Revise MI strategy to address previous recommendations	Fully Addressed	Fully Addressed
MI 3	Establish performance measures to assess ongoing progress	Fully Addressed	Fully Addressed
MI 4	Promote department-wide accountability through performance management system	Fully Addressed	Fully Addressed
	Fully Addressed GAO Outcomes (out of 30)	**18 (60%)**	**22 (73%)**
	Fully Addressed and Mostly Addressed GAO Outcomes (out of 30)	**22 (73%)**	**23 (77%)**

GAO Criteria	Definition	GAO Ratings as of 2023[3]
Leadership Commitment	Demonstrated strong commitment and top leadership support.	Met
Capacity	Agency has the capacity (i.e., people and resources) to resolve the risk(s).	Partially Met
Action Plan	A corrective action plan exists that defines the root cause, solutions, and provides for substantially completing corrective measures, including steps necessary to implement solutions [GAO] recommended.	Met
Monitoring	A program has been instituted to monitor and independently validate the effectiveness and sustainability of corrective measures.	Met
Demonstrated Progress	Ability to demonstrate progress in implementing corrective measures and in resolving the high-risk area.	Partially Met

Met or Fully Addressed	Mostly Addressed

[1] GAO Outcomes: GAO rates DHS's progress using the following scale: **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-21-119SP, page 180).

[2] On July 27, 2022, GAO provided DHS with updated outcome ratings which will be published in the 2023 update to the High-Risk List report.

[3] GAO did not advance the criteria ratings during the July meeting. Rating definitions are as follows: **Met** – Actions have been taken that meet the criterion. There are no significant actions that need to be taken to further address this criterion; **Partially Met** – Some, but not all, actions necessary to meet the criterion have been taken; **Not Met** – Few, if any, actions towards meeting the criterion have been taken. (Source: GAO-21-119SP, page 4).