



Inspector General

September 30, 2026

TO: Valorie Findlater
Chief of Management and Administration

FROM: William Brown
Acting Inspector General

SUBJECT: *Audit of NARA's Compliance with the Federal Information Security
Modernization Act (FISMA) for Fiscal Year 2026*
OIG Audit Report No. 26-AUD-09

The Office of Inspector General (OIG) contracted with Sikich CPA LLC (Sikich) to conduct an independent audit of the National Archives and Records Administration's (NARA's) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year 2026. Based on this year's FISMA requirements, which included assessing the maturity level of an agency's information security program across six function areas, Sikich determined that three function areas for NARA were at Maturity Level 2: *Defined*, two were at Maturity Level 3: *Consistently Implemented*, and one was at Maturity Level 4: *Managed and Measurable*. To be considered effective, NARA must receive an overall rating of Maturity Level 4: *Managed and Measurable* or higher.

Sikich concluded that NARA's information security program and practices are at Maturity Level 3: *Consistently Implemented* and therefore do not meet the requirements for an effective program under FISMA. The report contains six new recommendations and highlights existing open audit recommendations relevant to recurring security control weaknesses.

Sikich is responsible for the attached auditor's report dated September 29, 2026 and the conclusions expressed in the report. The findings and conclusions presented in the report are the responsibility of Sikich. The OIG's responsibility is to provide adequate oversight of the contractor's work in accordance with Generally Accepted Government Audit Standards.

Please provide planned corrective actions and expected dates to complete the actions for each of the recommendations within 30 days of the date of this report. As with all OIG products, we determine what information is publicly posted on our website from the published report. Consistent with our responsibility under the Inspector General Act of 1978, as amended, we may provide copies of our report to congressional committees with oversight responsibility for NARA. We appreciate the cooperation and assistance NARA extended to us during this audit. Please contact me with any questions.



■ National Archives and Records Administration

Performance Audit of the National Archives and Records Administration's
Implementation of the
Federal Information Security Modernization Act of 2014 for
Fiscal Year 2026

SEPTEMBER 29, 2026



333 John Carlyle Street, Suite 500
Alexandria, VA 22314
703.836.6701

September 29, 2026

William Brown
Acting Inspector General
Office of Inspector General
National Archives and Records Administration

Dear Mr. Brown:

Sikich CPA LLC (Sikich) is pleased to submit the attached report detailing the results of our performance audit of the National Archives and Records Administration's (NARA's) information security program and practices for Fiscal Year (FY) 2026 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires federal agencies to perform an annual independent evaluation of their information security program and practices. FISMA states that the evaluation is to be performed by the agency's Inspector General (IG) or by an independent external auditor, as determined by the IG. The NARA Office of the Inspector General engaged Sikich to conduct this performance audit.

The audit covered the period from October 1, 2025, through July 31, 2026. We performed audit fieldwork from March through July 2026.

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We describe our objective, scope, and methodology in **Appendix B: Objective, Scope, and Methodology**.

We appreciate the assistance provided by NARA management and staff.

Sincerely,

Sikich CPA LLC

Table of Contents

I.	Executive Summary	1
II.	Audit Results	5
	CSF Function: Govern	5
	CSF Function: Identify	8
	CSF Function: Protect.....	9
	CSF Function: Detect.....	15
	CSF Function: Respond.....	15
	CSF Function: Recover.....	16
	Appendix A: Background.....	17
	Appendix B: Objective, Scope, and Methodology.....	19
	Appendix C: Status of Prior-Year Recommendations	22
	Appendix D: Acronyms.....	27
	Appendix E: Management Comments.....	28
	OIG Hotline Contact Information	29

I. Executive Summary

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agencywide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also requires agency Inspectors General (IGs) to assess the effectiveness of their agency's information security program and practices. The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

The Office of the Inspector General (OIG) for the National Archives and Records Administration (NARA) engaged Sikich CPA LLC (Sikich) to conduct a performance audit in support of the FISMA requirement for an annual independent evaluation of NARA's information security program and practices. The objective of this performance audit was to determine the effectiveness of NARA's information security management program and practices.

OMB and the Department of Homeland Security (DHS) provide federal agencies and IGs with instructions for preparing FISMA reports. On January 15, 2025, OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*,¹ which provides reporting guidance for FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices. OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders collaborated to develop the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (IG FISMA Reporting Metrics).²

The IG FISMA Reporting Metrics require us to assess the maturity of six Cybersecurity Framework (CSF)³ functions in the agency's information security program and practices. For this year's review, the IG FISMA Reporting Metrics required IGs to assess 20 core⁴ and 5 supplemental⁵ metrics across 6 function areas—Govern, Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agency's information security program and the maturity level of each function area. The maturity levels are Level 1: *Ad Hoc*, Level 2: *Defined*, Level 3: *Consistently Implemented*, Level 4: *Managed and Measurable*, and Level 5: *Optimized*. To be considered effective, an agency's information security program must be rated Level 4:

¹ For FY 2026, OMB and DHS did not issue the annual FISMA instructions; therefore, we performed the audit using OMB M-25-04. See OMB M-25-04 online: [M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf](#).

² On March 17, 2026, OMB and CIGIE issued a joint communication directing IGs and independent external auditors to use the FY 2025 IG FISMA Reporting Metrics for FY 2026 FISMA audits. See the IG FISMA Reporting Metrics online: [FY 2025 Inspector General Federal Information Security Modernization Act of 2014 \(FISMA\) Reporting Metrics v2.0](#).

³ The IG FISMA Reporting Metrics align with the six functions in the NIST Cybersecurity Framework 2.0 (Cybersecurity Framework): *Govern, Identify, Protect, Detect, Respond, and Recover*. The CSF provides agencies with a common structure for managing and reducing their cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.

⁴ Core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine the effectiveness of a security program. The core metrics can be found in the IG FISMA Reporting Metrics online: [FY 2025 Inspector General Federal Information Security Modernization Act of 2014 \(FISMA\) Reporting Metrics v2.0](#).

⁵ Supplemental metrics are not considered core metrics, but represent important activities conducted by security programs and contribute to the overall evaluation and determination of the effectiveness of the security program. The supplemental metrics can be found in the IG FISMA Reporting Metrics online: [FY 2025 Inspector General Federal Information Security Modernization Act of 2014 \(FISMA\) Reporting Metrics v2.0](#).

Managed and Measurable or higher.⁶ See **Appendix A** for background information on the FISMA reporting requirements.

For this audit, Sikich reviewed selected controls from NIST Special Publication (SP) 800-53, Revision (Rev.) 5, *Security and Privacy Controls for Information Systems and Organizations*, which support the IG FISMA Reporting Metrics, for a sample of 6 out of 40⁷ information systems⁸ in NARA's FISMA reportable system inventory as of March 25, 2026. The audit covered the period from October 1, 2025, through July 31, 2026. We performed the audit fieldwork from March to July 2026.

We concluded that NARA's information security program and practices did not meet the requirements to be considered effective. Specifically, NARA's information security program and practices are at Maturity Level 3: *Consistently Implemented*. To be considered effective, an agency's information security program must be rated at Maturity Level 4: *Managed and Measurable* or higher. **Table 1** below summarizes NARA's overall assessed maturity levels for each CSF function and domain in the IG FISMA Reporting Metrics. We determined that one CSF function was rated at Maturity Level 4: *Managed and Measurable*, two CSF functions were rated at Maturity Level 3: *Consistently Implemented*, and three CSF functions were rated at Maturity Level 2: *Defined*.

Table 1: Maturity levels for IG FISMA Reporting Metrics

CSF Functions ⁹	Maturity Level by Function	Domain	Maturity Level by Domain
Govern	Level 2: <i>Defined</i>	Cybersecurity Governance	Level 2: <i>Defined</i>
		Cybersecurity Supply Chain Risk Management (C-SCRM)	Level 2: <i>Defined</i>
Identify	Level 2: <i>Defined</i>	Risk and Asset Management	Level 2: <i>Defined</i>
Protect	Level 2: <i>Defined</i>	Configuration Management	Level 2: <i>Defined</i>
		Identity and Access Management	Level 2: <i>Defined</i>
		Data Protection and Privacy	Level 2: <i>Defined</i>
		Security Training	Level 2: <i>Defined</i>
Detect	Level 4: <i>Managed and Measurable</i>	Information Security Continuous Monitoring	Level 4: <i>Managed and Measurable</i>
Respond	Level 3: <i>Consistently Implemented</i>	Incident Response	Level 3: <i>Consistently Implemented</i>
Recover	Level 3: <i>Consistently Implemented</i>	Contingency Planning	Level 3: <i>Consistently Implemented</i>
Overall	Level 3: <i>Consistently Implemented</i>		

Source: Sikich's assessment of NARA's information security program controls and practices based on the IG FISMA Reporting Metrics

⁶ According to the IG FISMA Reporting Metrics, "the OMB believes that achieving a Level 4 (Managed and Measurable) or above represents an effective level of security."

⁷ NARA's population of FISMA reportable systems included 43 systems as of March 25, 2026. We further refined that population to exclude OIG, Top Secret and Title 13 systems, resulting in a population of 40 systems for our sample selection.

⁸ According to the [NIST Glossary](#), an information system is "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

⁹ See Appendix A, Tables 3 and 4, for the definitions and explanations of the CSF functions and domains and the IG FISMA Reporting Metrics maturity levels, respectively.

While NARA's information security program and practices did not meet the requirements to be considered effective in accordance with FISMA, their current Maturity Level 3: *Consistently Implemented* has improved from last year's rating. We noted that NARA has established several information security program controls and practices that are consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. For example, NARA has taken the following actions:

- Developed cybersecurity risk profiles.
- Implemented role-based privacy training.
- Enforced Personal Identity Verification (PIV) authentication for non-privileged NARANet users.
- Strengthened the authorization process for its systems using automated mechanisms.

Notwithstanding these actions, this report describes new and repeat security control weaknesses that reduced the effectiveness of NARA's information security program and practices. To fully progress toward an effective information security program, NARA must address the new and repeat weaknesses in its information security program related to the Cybersecurity Governance, C-SCRM, Risk and Asset Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains of the IG FISMA Reporting Metrics.

In addition, NARA has outstanding open audit recommendations from prior years that impact its ability to improve this year's IG FISMA Reporting Metrics maturity levels. Specifically, at the beginning of the FY 2026 FISMA audit, NARA had 27 open recommendations from prior FISMA audits for 2023,¹⁰ 2024,¹¹ and 2025.¹² During the FY 2026 FISMA audit, NARA took corrective actions to address 12¹³ of these recommendations, and we consider those recommendations closed. Corrective actions are in progress for the 15 open recommendations.

Some of the recurring security weaknesses continue to present significant risk to NARA, including unsupported software, missing patches, weak passwords, and configuration weaknesses. In addition, given NARA's continued weak password configurations, we were able to exploit certain vulnerabilities to obtain unauthorized elevated domain account permissions/privileges and access system resources.¹⁴ As a result, these weaknesses may enable malicious actors to gain unauthorized access to mission-critical systems and data.

The prior-year control weaknesses, along with the new control weaknesses identified (as summarized below in **Table 2**), affect NARA's ability to preserve the confidentiality, integrity, and availability of its information and information systems, potentially exposing its information and information systems to unauthorized access, use, disclosure, or modification. As a result, we made six new recommendations to assist NARA in strengthening its information security program and practices.

¹⁰ *National Archives and Records Administration's Fiscal Year 2023 Federal Information Security Modernization Act of 2014 Audit* (OIG Report No. 24-AUD-01, October 24, 2023).

¹¹ *National Archives and Records Administration's Fiscal Year 2024 Federal Information Security Modernization Act of 2014 Audit* (OIG Audit Report No. 24-AUD-07, September 27, 2024).

¹² *Audit of NARA's Compliance with the Federal Information Security Modernization Act (FISMA) for Fiscal Year 2025* (OIG Audit Report No. 25-AUD-08, September 30, 2025).

¹³ See Appendix C for the status of prior-year recommendations.

¹⁴ Management Alert: *Cybersecurity Vulnerabilities Identified During the Fiscal Year (FY) 2026 FISMA Audit – NARA Internal Penetration Testing* (OIG Report 26-R-05, June 30, 2026).

Table 2: IG FISMA Metric Domains Mapped to Current Weaknesses

IG FISMA Metric Domain	Weaknesses Noted
Cybersecurity Governance	NARA has not defined its policies and procedures for creating and maintaining current or target cybersecurity postures and its enterprise risk management strategy does not include current cybersecurity risk attributes.
C-SCRM	NARA has not formalized policies and procedures for C-SCRM.
Risk and Asset Management	Prior-year weaknesses related to review and update of Information Technology (IT) policies and procedures and hardware asset inventory management remained open.
Configuration Management	Critical and high-risk security vulnerabilities persist related to patch management, configuration management, unsupported software, and weak authentication mechanisms. In addition, we noted weaknesses in baseline configuration settings.
Identity and Access Management	Weaknesses related to inactive accounts persist. In addition, prior-year weaknesses primarily related to continued implementation of multifactor authentication and account management controls remained open.
Data Protection and Privacy	We noted weaknesses in NARA's encryption of sensitive data at rest controls. In addition, prior-year weaknesses related to privacy impact assessments and deprecated encryption protocols remained open.
Security Training	NARA has not completed their annual cybersecurity workforce assessment. In addition, a prior-year weakness related to the completeness of new hire security awareness remained open.
Information Security Continuous Monitoring	No weaknesses noted.
Incident Response	No weaknesses noted.
Contingency Planning	No weaknesses noted.

Source: Sikich's assessment of NARA's information security program controls and practices based on the IG FISMA Reporting Metrics.

The following section provides a detailed discussion of the audit results. **Appendix A** provides background information on FISMA. **Appendix B** describes the audit objective, scope, and methodology. **Appendix C** provides the status of prior-year recommendations. **Appendix D** provides a listing of acronyms used throughout this report. **Appendix E** contains management's comments on the report.

II. Audit Results

This section describes the key controls underlying each function and domain and our assessment of NARA's implementation of those controls. We have organized our conclusions and ratings by function area and domain to help orient the reader to deficiencies as categorized by NIST's CSF.

CSF Function: Govern

The objective of the Govern function is to establish, communicate, and monitor an organization's cybersecurity risk management strategy, expectations, and policy. We determined that the maturity level of NARA's Govern function is Level 2: *Defined*.

Metric Domain: Cybersecurity Governance

An agency with an effective cybersecurity governance program (1) monitors and reports on its progress in reaching target profiles and refines its organizational profiles periodically based on known risk exposure; (2) uses qualitative and quantitative data to assess the effectiveness of its cybersecurity risk management and integrates the cybersecurity risk management program into the organization's enterprise risk management strategy; and (3) ensures that it has allocated adequate resources commensurate with cybersecurity responsibilities and uses qualitative and quantitative performance measures on the effectiveness of cybersecurity risk management roles.

We determined that the maturity level of NARA's Cybersecurity Governance domain is Level 2: *Defined*. We identified weaknesses related to NARA's policies and procedures for creating and maintaining cybersecurity profiles, as well as its cybersecurity risk appetite and risk tolerance statements, as discussed below:

Cybersecurity Profile Policies and Procedures

NARA has not defined its policies and procedures for creating and maintaining current or target cybersecurity postures that, at a minimum, consider the agency's mission objectives, threat landscape, resources (including personnel), and operational constraints. Although NARA uses guidance and templates from NIST SP 1301: *CSF 2.0: Quick-Start Guide for Creating and Using Organizational Profiles* (February 26, 2024), to develop current and target profiles using the CSF 2.0 Profile Template, this guidance is not sufficient substitute for agency-specific policies and procedures.

NARA indicated that they relied upon NIST SP 1301 guidance and templates in lieu of developing agency-specific policies and procedures governing the creation, review, maintenance, and approval of current and target organizational profiles.

The NIST CSF 2.0 (February 26, 2024) states that an organization may benefit from using the CSF as guidance to help it understand, assess, prioritize, and communicate cybersecurity risks and the actions that will manage those risks. The selected outcomes can be used to focus on and implement strategic decisions to improve cybersecurity postures and maintain continuity of mission-essential functions while taking priorities and available resources into account.

Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), states:

Each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework)¹⁵ developed by NIST, or any successor document, to manage the agency's cybersecurity risk.

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (May 2025), GAO-25-107721, *Principle 12 – Implement Control Activities*, states:

12.01 – Management should implement control activities through policies and procedures.

12.02 – Management establishes control activities by documenting in policies what is expected and in procedures specified actions that implement policies, to mitigate risks to achieving the entity's objectives to acceptable levels [documentation requirement].

Although NARA has completed an Office of the Chief Information Officer (OCIO) Cybersecurity Profile and plans to update it annually, the lack of formalized policies and procedures increases the risk that roles, responsibilities, and milestones may not be consistently communicated, implemented and achieved.

Recommendation:

1. We recommend that the NARA Chief Information Officer document and implement policies and procedures for the development, review, and maintenance of current and target cybersecurity profiles that, at a minimum, consider NARA's mission objectives, threat landscape, available resources (including personnel), and organizational constraints.

Cybersecurity Risk Appetite and Risk Tolerance

NARA's enterprise risk management strategy does not include current cybersecurity risk attributes. This occurred because NARA has not yet developed a cybersecurity risk appetite¹⁶ and risk tolerance statement.¹⁷

The NIST CSF 2.0 (February 26, 2024), states, in part:

GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

...

- *Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.*

¹⁵ Before version 2.0, the Cybersecurity Framework was called the *Framework for Improving Critical Infrastructure Cybersecurity*. This title is not used for NIST CSF 2.0.

¹⁶ OMB Circular A-123, *Management's Responsibility for Internal Control*, states that an agency's risk appetite may vary by the type of risk and the mission of the organization. Risk appetite articulates the level and type of risk the agency will accept while conducting its mission and carrying out its strategic plan.

¹⁷ OMB Circular A-123, states that risk tolerance is the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite. Managing the risks associated with achieving an organization's mission through its objectives requires an assessment of these risks.

- ...
- *GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained.*

OMB Circular A-123, *Management's Responsibility for Internal Control* (March 10, 2026), Section B. Requirements for an Effective System of Internal Control Implementation, Agency Leadership Requirements, states:

2. Risk Assessment: Clearly define the agency's objectives and develop risk appetite and tolerance levels.

Without a documented cybersecurity risk appetite and risk tolerance statement, NARA increases the likelihood that cybersecurity risks will not be adequately identified, assessed, and incorporated into its Enterprise Governance, Risk, and Compliance Program.

Recommendation:

2. We recommend that the NARA Chief Information Officer, in coordination with the Chief Financial Officer, establish, document, and maintain cybersecurity risk appetite and risk tolerance statements and integrate them into NARA's Enterprise Governance, Risk, and Compliance Program.

Metric Domain: Cybersecurity Supply Chain Risk Management

An agency with an effective C-SCRM program (1) reports qualitative and quantitative performance measures on the effectiveness of its supply chain risk management program and (2) has incorporated supplier risk evaluations into its continuous monitoring practices.

We determined that the maturity level of NARA's C-SCRM domain is Level 2: *Defined* and identified the following weakness:

NARA has not formalized policies and procedures for C-SCRM to ensure that NARA-defined systems including system components, and services adhere to C-SCRM requirements.

Specifically, we noted that while NARA has developed and communicated a C-SCRM strategy and developed a C-SCRM implementation plan, it is still in the process of implementing key components. These components include the development of policies and procedures, creation of a C-SCRM governance board, and a C-SCRM office charter.

According to NARA management, the development of C-SCRM policies and procedures has not yet started due to reorganization efforts and a government shutdown earlier in the fiscal year. In addition, management indicated that the scope of NARA's implementation will likely change due to changes in the Federal Acquisition Regulation to include standard language for C-SCRM within the federal government related to acquisition efforts.

The NIST CSF 2.0 (February 26, 2024), states:

GV: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

...

- *GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.*

The GAO's *Standards for Internal Control in the Federal Government* (May 2025), GAO-25-107721, *Principle 12 – Implement Control Activities*, states:

12.01 – Management should implement control activities through policies and procedures.

12.02 – Management establishes control activities by documenting in policies what is expected and in procedures specified actions that implement policies, to mitigate risks to achieving the entity's objectives to acceptable levels [documentation requirement].

Without formalized C-SCRM policies and procedures, NARA risks inconsistent implementation of controls and unclear assignment of responsibilities for products, system components, systems, and services.

Recommendation:

3. We recommend that the NARA Chief Information Officer establish and implement C-SCRM policies and procedures to ensure that NARA-defined systems, including system components, and services comply with C-SCRM requirements.

CSF Function: Identify

The objective of the Identify function is to ensure that the organization understands its cybersecurity risks. We determined that the maturity level of NARA's Identify function is Level 2: *Defined*.

Metric Domain: Risk and Asset Management

An agency with an effective risk and asset management program maintains an accurate inventory of information systems, hardware assets, and software assets; consistently implements its risk management policies, procedures, plans, and strategy at all levels of the organization; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its risk and asset management program.

We determined that the maturity level of NARA's Risk and Asset Management domain is Level 2: *Defined*. NARA has not fully implemented components of its agency-wide information security risk and asset management program that are necessary to meet FISMA requirements. Specifically, NARA has two open prior-year recommendations in the Risk and Asset Management domain.¹⁸ These weaknesses relate to (1) the review and approval of IT policies, procedures, methodologies, and supplements in accordance with NARA Directive 111, *NARA Directives*, and (2) hardware asset inventory management.

¹⁸ Recommendations 1 and 3 (OIG Audit Report No. 24-AUD-07, September 27, 2024). See Appendix C for additional information regarding these prior-year recommendations. We are not repeating these recommendations within this report.

Recommendation:

We recommend that the NARA Chief Information Officer take actions to address the open prior-year recommendations related to the Risk and Asset Management domain.¹⁹

CSF Function: Protect

The objective of the Protect function is to ensure that organizations use safeguards to manage their cybersecurity risks. We determined that the maturity level of NARA's Protect function is Level 2 *Defined*.

NARA's Protect controls—which cover configuration management, identity and access management, data protection and privacy, and security training—were not effective, and NARA did not consistently implement the controls organization-wide. In 2026, weaknesses in NARA's IT environment continued to contribute to deficiencies in system configurations, access controls, and data protection and privacy controls.

Metric Domain: Configuration Management

An agency with an effective configuration management program employs automation to maintain an accurate view of the security configurations for all information system components connected to the agency's network; centrally manages its flaw remediation process; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its configuration management program.

We determined that the maturity level of NARA's Configuration Management domain is Level 2: *Defined*. We noted that NARA has four open prior-year recommendations in the Configuration Management domain²⁰ that relate to improving its vulnerability management program.

In addition, the independent vulnerability assessment and penetration test we performed during the FY 2026 FISMA audit identified issues similar to those addressed in the open prior-year recommendations related to NARA's vulnerability management program, including vulnerabilities related to patch management, configuration management, unsupported software, and weak passwords. The audit also identified weaknesses related to baseline configurations, as discussed below.

Baseline Configurations

NARA has not fully implemented their defined baseline configuration settings. Specifically, we noted baseline compliance percentages for NARA devices ranged from 34.7 percent to 93.7 percent.

NARA management stated that the current baseline compliance percentages do not account for approved deviations. Management also noted that NARA is working to incorporate these approved deviations into its baseline compliance scanning tool to provide a more accurate representation of device compliance and enable remediation efforts to focus on actual baseline compliance failures.

¹⁹ Prior FISMA open recommendations related to the Risk and Asset Management domain include Recommendations 1 and 3 (OIG Audit Report No. 24-AUD-07, September 27, 2024). See Appendix C for additional information regarding these prior-year recommendations. We are not repeating these recommendations within this report.

²⁰ Recommendations 2, 3, and 4 (OIG Audit Report No. 25-AUD-08, September 30, 2025) and Recommendation 6 (OIG Audit Report No. 24-AUD-07, September 27, 2024). See Appendix C for additional information regarding these prior-year recommendations.

The *NARANet General Support System Common Controls System Security Plan* (September 9, 2025), control CM-6, states the following regarding baseline configuration settings:

(a) Establishes and documents configuration settings for information technology products employed within the information system using Security Architecture security configuration checklists approved and published by NARA IT Security Management Division (IS) that reflect the most restrictive mode consistent with operational requirements;

(b) Implements the configuration settings;

Noncompliance with established baseline configurations increases the risk of misconfigured and insecure systems, reducing NARA's ability to consistently protect its information systems and increasing the likelihood of system compromise.

Recommendations:

4. We recommend that the NARA Chief Information Officer update the defined baseline configuration settings for all devices.
5. We recommend that the NARA Chief Information Officer implement the baseline compliance scanning tool to account for approved deviations.

Vulnerability Management Program and Processes

We compared the NARA workstation vulnerability scan results from March 2026 and April 2026 to determine whether NARA was remediating high and critical severity vulnerabilities within required timeframes. We identified 116 critical and high severity vulnerabilities that were not remediated between the two months. As a result, vulnerabilities have not been remediated within the defined timeframes.

In addition, we performed a penetration test from the internal NARA's network and identified weaknesses related to weak and reused passwords, and shared files which were accessible without authentication. We were able to use those password weaknesses to obtain unauthorized access to accounts with administrator access. We were then able to use the compromised accounts to create new domain administrator accounts.²¹

NARA is in the process of implementing corrective actions for a prior-year recommendation related to patch and vulnerability management. At the time of our assessment, NARA had not yet completed its corrective actions.

These weaknesses also occurred because NARA did not review service account passwords to determine whether each account had a unique password, did not review domain user accounts to determine if the accounts had weak passwords, and did not disable non-essential certificate services, endpoints, or web enrollment services.

The *NIST System Security Plan for NARANet General Support System Common Controls* (September 9, 2025), states the following with regard to security control Risk Assessment (RA-5): Vulnerability Scanning:

²¹ Management Alert: *Cybersecurity Vulnerabilities Identified During the Fiscal Year (FY) 2026 FISMA Audit – NARA Internal Penetration Testing* (OIG Report 26-R-05, June 30, 2026).

(d) Remediates legitimate vulnerabilities within NARA-defined timeframes of 30 days (Critical, High) and 60 days (Moderate, Low) in accordance with an organizational assessment of risk;

Missing patches, unsupported software, and configuration weaknesses increase the risk of an attacker exploiting these vulnerabilities to gain unauthorized access to sensitive information, resulting in information loss or disclosure.

Furthermore, reusing passwords, especially weak or default passwords, increases the risk of compromise. If a malicious actor compromises an account with elevated privileges, such as the account of a system administrator, the magnitude of harm increases, as the attacker can upload malware, steal sensitive data, add or delete users, change system configurations, and alter logs to conceal their actions. If several accounts use the same weak password, a malicious actor could leverage multiple accounts to further obfuscate their activities.

Recommendations:

We recommend that the NARA Chief Information Officer take actions to address open prior-year weaknesses identified in the Configuration Management domain related to the vulnerability management program.²²

Metric Domain: Identity and Access Management

An agency with an effective identity and access management program ensures that all privileged and non-privileged users employ strong authentication for accessing organizational systems and uses automated mechanisms to assist in managing privileged accounts.

We determined that the maturity level of NARA's Identity and Access Management domain is Level 2: *Defined*. We found that NARA had opportunities to improve its identity and access management program by implementing the five open prior-year recommendations in this area.²³ These recommendations primarily relate to the continued implementation of multifactor authentication and account management controls.

In addition, during the current year's audit, we identified similar weaknesses related to inactive accounts, as detailed below.

Account Management Controls

NARA had not disabled inactive NARANet administrator accounts that are no longer needed or that present least privilege concerns. Specifically, based on a review of NARANet administrator accounts, we found that 28 accounts had not logged in for more than 60 days. Of these, NARA determined that 13 accounts were either no longer needed or posed least privilege concerns.²⁴

NARA introduced and configured accounts to serve specifically as local workstation administrator accounts. These were restricted to Tier II Support and selected members of the

²² Open prior-year FISMA recommendations related to the findings noted within the Configuration Management domain include Recommendations 2, 3, and 4 (OIG Audit Report No. 25-AUD-08, September 30, 2025) and Recommendation 6 (OIG Audit Report No. 24-AUD-07, September 27, 2024). See Appendix C for additional information regarding these recommendations. We are not repeating these recommendations within this report.

²³ Recommendations 5, 9, and 15 (OIG Audit Report No. 24-AUD-07, September 27, 2024) and Recommendations 12 and 14 (OIG Audit Report No. 24-AUD-01, October 24, 2023). See Appendix C for additional information regarding these prior-year recommendations. We are not repeating these recommendations within this report.

²⁴ As a result, NARA initiated service desk tickets to disable these accounts.

Tier III System Engineering Team to enforce the principle of least privilege during troubleshooting and maintenance.

However, due to the distinct operational roles within the System Engineering Team, several members did not require regular use of these local workstation administrator rights. Consequently, those specific accounts exceeded the 60-day inactivity threshold. Following an internal review of account utilization, it was determined that these specific inactive accounts were no longer operationally necessary.²⁵

NARA User Account and Privileged User Account Management Standard Operating Procedure (SOP), Version 10 (January 2026), states, "All accounts will be disabled after 60 days and de-provisioned after 90 days."

In addition, Section 5.27, *Account Deprovision Procedure*, states:

When an account has been inactive for over 30 days, the NITTSS [NARA Information Technology and Telecommunications Support Services] will notify NARA IO [Information Owner] with the user's name. After 60 days, the user will be disabled, and after 90 days, the user will be de-provisioned. If a user has been de-provisioned for over 180 days, they will be removed from the system.

If NARA does not disable administrator accounts in a timely manner when no longer needed, there is an increased risk that unauthorized individuals may access these accounts.

Recommendation:

We recommend that the NARA Chief Information Officer take actions to address open prior-year recommendations related to the weaknesses noted for the Identity and Access Management domain.²⁶

Metric Domain: Data Protection and Privacy

An agency with an effective data protection and privacy program maintains the confidentiality, integrity, and availability of its data; can assess its security and privacy controls, as well as its breach response capabilities; and reports on qualitative and quantitative data protection and privacy performance measures.

We determined that the maturity level of NARA's Data Protection and Privacy domain is Level 2: *Defined*. NARA has three open prior-year recommendations in this area related to completing privacy impact assessments and data encryption.²⁷ In addition, during the current year's audit, we identified similar issues related to encryption controls, as detailed below.

²⁵ As a result, NARA has disabled and removed the inactive workstation administrator accounts for the affected System Engineering team members.

²⁶ Open prior-year recommendations related to the findings noted within the Identity and Access Management domain include Recommendations 5, 9, and 15 (OIG Audit Report No. 24-AUD-07, September 27, 2024) and Recommendations 12 and 14 (OIG Audit Report No. 24-AUD-01, October 24, 2023). See Appendix C for additional information regarding these prior-year recommendations. We are not repeating these recommendations within this report.

²⁷ Open prior-year recommendations noted within the Data Protection and Privacy domain include Recommendation 15 (OIG Audit Report No. 24-AUD-01, October 24, 2023) and Recommendations 5 and 6 (OIG Audit Report No. 25-AUD-08, September 30, 2025). See Appendix C for additional information regarding these prior-year recommendations. We are not repeating these recommendations within this report.

Encryption Controls

We noted that NARA's encryption of data at rest has not been fully implemented. For example, based on NARA's 2025 Chief Information Officer FISMA Q4/Annual Report submission, 10 of 41 systems (which store sensitive data) do not encrypt sensitive data. Additionally, we noted the following:

- Full disk encryption was not enabled on devices running a specific operating system.
- Data encryption at rest was not enabled on 54 of 4,366 NARA end user devices.

For the devices without data encryption enabled, these devices are either not getting the proper group policy object applied for data encryption enablement, or they are devices that are still registered as objects within active directory but are not actually deployed and live currently.

NARA IT Security Requirements, version 7.5 (June 12, 2025), SC-28: *Protection of Information at Rest*, states:

The system shall protect the integrity and confidentiality by encrypting data at rest in accordance with FIPS [Federal Information Processing Standards] 140-2.

NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (December 10, 2020), System and Communications Protection, SC-28(1), *Protection of Information at Rest | Cryptographic Protection*, requires:

The organization to implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].

Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), Section 3 Modernizing Federal Government Cybersecurity, states:

(d) Within 180 days of the date of this order, agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws.

Without implementing data encryption there is an increased risk of unauthorized disclosure or modification of sensitive data.

Recommendation:

We recommend that the NARA Chief Information Officer take actions to address open prior-year recommendations related to the weaknesses noted for the Data Protection and Privacy domain.²⁸

Metric Domain: Security Training

An agency with an effective security training program identifies and addresses gaps in security knowledge, skills, and abilities through training or talent acquisition.

²⁸ Open prior-year recommendations noted within the Data Protection and Privacy domain include Recommendation 15 (OIG Audit Report No. 24-AUD-01, October 24, 2023) and Recommendations 5 and 6 (OIG Audit Report No. 25-AUD-08, September 30, 2025). See Appendix C for additional information regarding these prior-year recommendations. We are not repeating these recommendations within this report.

We determined that the maturity level of NARA's Security Training domain is Level 2: *Defined*. NARA has one open prior-year recommendation in this area related to enhancing procedures to ensure that NARA automatically disables accounts for new NARA users who do not complete their initial security awareness training in accordance with the timeframes promulgated within the Privacy and Awareness Handbook.²⁹ In addition, NARA has not completed their annual cybersecurity workforce assessment, as discussed below.

Workforce Assessment

NARA has not completed an annual cybersecurity workforce assessment. Specifically, NARA's cybersecurity workforce assessment is intended to be performed as part of its annual training plan. However, in response to our request for the most recent cybersecurity workforce assessment, we received NARA's 2025 Chief Information Officer FISMA Q4/Annual Report submission. While these metrics identify the number of roles requiring specialized training, they do not represent an annual cybersecurity workforce assessment.

Since NARA did not develop an FY 2026 training plan, it did not conduct a cybersecurity workforce assessment to identify role-based training needs, evaluate cybersecurity skills gap, or align workforce capabilities with the agency's risk profile.

NARA Awareness and Training (AT) Handbook (August 15, 2022), version 1.1, states:

5.1.2. Role Assessment

IS [Information Services] performs an annual assessment of the NARA workforce during the development of the Annual CPATP [Cybersecurity and Privacy Awareness and Training Program] to determine the roles requiring specialized training and the LMS [Learning Management System] Skillsoft or FedVTE [Federal Virtual Training Environment] course to be selected for the current year. IS performs an analysis of metrics from the previous year's awareness and training to better understand the skills, knowledge, and abilities of its workforce to determine the roles for requiring specialized training and the selected FedVTE course.

OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016), Section 5. Policy, c. Leadership and Workforce, requires agencies to maintain a current workforce planning process to ensure that the agency can anticipate and respond to changing mission requirements and maintain workforce skills in a rapidly developing information technology environment.

Without a current cybersecurity workforce assessment, NARA is not able to identify missing or weak proficiencies across key cybersecurity domains, reducing the risk of security incidents occurring by not addressing capability gaps. In addition, the workforce assessment enables targeted training ensuring teams have the necessary knowledge and abilities to respond to cybersecurity threats.

²⁹ Recommendation 11 (OIG Audit Report No. 24-AUD-01, October 24, 2023). We are not repeating this recommendation within this report.

Recommendation:

We recommend that the NARA Chief Information Officer take the following action related to the weakness identified in the Security and Training domain, in addition to addressing the open-prior-year recommendation.³⁰

6. Perform and document the annual assessment of NARA's cybersecurity workforce during the development of the annual CPATP to ensure the roles requiring specialized training and courses are selected for the year.

CSF Function: Detect

The objective of the Detect function is to ensure that organizations identify and analyze possible cybersecurity attacks and compromises. We determined that the maturity level of NARA's Detect function is Level 4: *Managed and Measurable*.

Metric Domain: Information Security Continuous Monitoring

An agency with an effective information security continuous monitoring program maintains ongoing authorizations of information systems; uses up-to-date cyber threat intelligence when analyzing logs; automates its inventory collection and anomaly detection to detect unauthorized devices; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its information security continuous monitoring policies, procedures, plans, and strategies.

We determined that the maturity level of NARA's Information Security Continuous Monitoring domain is Level 4: *Managed and Measurable*.

NARA has defined and consistently implemented processes for performing ongoing information security assessments with regard to granting system authorizations, including developing security plans and monitoring system security controls. In addition, NARA has implemented several automated analysis tools for incident response, and utilizes the Security Operations Center as a Service through the Department of Justice's Cybersecurity Shared Services to provide additional real-time incident response capabilities.

CSF Function: Respond

The objective of the Respond function is to ensure that organizations take action regarding detected cybersecurity incidents. We determined that the maturity level of NARA's Respond function is Level 3: *Consistently Implemented*.

Metric Domain: Incident Response

An agency with an effective incident response program:

- Uses profiling techniques to measure the characteristics of expected network and system activities so it can more effectively detect security incidents.
- Manages and measures the impact of successful incidents.
- Uses incident response metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

³⁰ An open prior-year FISMA recommendation related to the Security Training domain includes Recommendation 11 (OIG Audit Report No. 24-AUD-01, October 24, 2023). See Appendix C for additional information regarding this prior-year recommendation. We are not repeating this recommendation within this report.

- Consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies.
- Meets event logging maturity requirements.

We determined that the maturity level for NARA's Incident Response domain is Level 3: *Consistently Implemented*. NARA has established and consistently implemented policies and procedures for identifying, managing, and responding to cybersecurity incidents. However, NARA has not consistently implemented its security information and event management tool across all FISMA reportable systems or developed a network that can perform automated actions to misdirect attackers, as required to achieve a higher maturity level for the Incident Response domain.

CSF Function: Recover

The objective of the Recover function is to ensure that organizations restore assets and operations affected by a cybersecurity incident. We determined that the maturity level of NARA's Recover function is Level 3: *Consistently Implemented*.

Metric Domain: Contingency Planning

An agency with an effective contingency planning program ensures that it integrates the results of business impact analyses with its enterprise risk management processes and uses these results to make senior-level decisions; employs automated mechanisms to thoroughly and effectively test system contingency plans; and communicates metrics on the effectiveness of recovery activities to relevant stakeholders.

We determined that the maturity level of NARA's Contingency Planning domain is Level 3: *Consistently Implemented*. We noted that NARA has no open prior-year recommendations in the Contingency Planning domain.

NARA has defined and consistently implemented business impact analyses and contingency plans for all sampled systems. Although NARA has consistently implemented contingency planning processes, it did not demonstrate that it measures the effectiveness of these processes. Specifically, NARA did not demonstrate (1) how it uses the results of business impact analyses in conjunction with its risk register to calculate potential losses and inform senior-level decisions or (2) that it uses automated mechanisms to test contingency plans more thoroughly and effectively. As a result, NARA has not yet achieved a higher maturity level for the Contingency Planning domain.

Appendix A: Background

Federal Information Security Modernization Act of 2014

FISMA requires federal agencies to develop, document, and implement an agencywide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. Agencies must also report annually to OMB and congressional committees on the effectiveness of their information security program and practices. In addition, FISMA requires agency IGs to assess the effectiveness of their agency's information security program and practices.

NIST Security Standards and Guidelines

FISMA requires NIST to provide standards and guidelines pertaining to federal information systems. The standards prescribed include information security standards that provide the minimum information security requirements necessary to improve the security of federal information and information systems. FISMA also requires that federal agencies comply with the Federal Information Processing Standards issued by NIST. In addition, NIST develops and issues SPs as recommendations and guidance documents.

FISMA Reporting Requirements

OMB and DHS provide federal agencies and IGs with instructions for preparing FISMA reports. On January 15, 2025, OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, which provides reporting guidance for FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices. OMB, CIGIE, and other stakeholders collaborated to develop these metrics.

As highlighted in **Table 3**, the IG FISMA Reporting Metrics are designed to assess the maturity of an agency's information security program and practices and align with the six function areas in NIST CSF: Govern, Identify, Protect, Detect, Respond, and Recover.

Table 3: Alignment of the CSF Functions to the Domains in the IG FISMA Reporting Metrics

CSF Functions	Function Area Objective	Domain(s)
Govern	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	Cybersecurity Governance and C-SCRM
Identify	The organization's current cybersecurity risks are understood.	Risk and Asset Management
Protect	Safeguards to manage the organization's cybersecurity risks are used.	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Possible cybersecurity attacks and compromises are found and analyzed.	Information Security Continuous Monitoring
Respond	Actions regarding a detected cybersecurity incident are taken.	Incident Response
Recover	Assets and operations affected by a cybersecurity incident are restored.	Contingency Planning

Source: Sikich's analysis of NIST CSF and the IG FISMA Reporting Metrics

The foundational levels of the maturity model in the IG FISMA Reporting Metrics focus on developing sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 4** below explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of at least Level 4: *Managed and Measurable*.

Table 4: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: IG FISMA Reporting Metrics

Appendix B: Objective, Scope, and Methodology

Objective

The objective of this performance audit was to determine the effectiveness of NARA's information security management program and practices.

Scope

The scope of this performance audit covered NARA's information security program and practices, consistent with FISMA and reporting instructions that OMB and DHS issued for FY 2026. The scope also included assessing selected controls from NIST SP 800-53, Rev. 5, which support the IG FISMA Reporting Metrics, for a sample of 6 out of 40 information systems³¹ in NARA's FISMA reportable system inventory as of March 25, 2026 (**Table 5**).

Table 5: Description of the Systems Selected for Testing

System Name	System Description
NARANet	General support system which consists of all the hardware, operating systems and connectivity to NARA-networked devices.
Order Fulfillment Accounting System (OFAS)	Financial management system that tracks and provides accounting of customer service requests for reproductions of NARA holdings and other NARA products.
Record Center Processing Billing System (RCPBS)	Supports records center programs in producing invoices for the storage and servicing of NARAs Regional Record Centers.
Insider Threat Program Support System (ITPSS)	Supports the NARA data collection and analysis of machine data related to insider threat monitoring activities.
Agency Digital Asset Management Systems (ADAMS)	Provide a comprehensive, agency-wide approach for collecting and managing digital and legacy agency special media assets.
Next Generation Case Management and Reporting System (NextGen CMRS)	CMRS provides improved workload management and processes related to fulfilling requests for military records.

Source: NARA System Inventory

In addition, we assessed NARA's technical controls by performing an internal and external vulnerability assessment and penetration test covering a subset of NARA information systems in scope for the audit. We conducted these vulnerability assessment and penetration tests to determine the effectiveness of controls that prevent or detect unauthorized access, disclosure, modification, or deletion of sensitive information. We incorporated the results of the internal vulnerability assessment and penetration tests into our FISMA audit results.

For this year's review, IGs were required to assess 20 core and 5 supplemental metrics across 6 function areas—Govern, Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agency's information security program and the maturity level of each function area.

The audit also included an evaluation of whether NARA took corrective actions to address open recommendations from prior FISMA audits. See **Appendix C** for the status of the prior-year recommendations.

³¹ NARA's population of FISMA reportable systems included 43 systems as of March 25, 2026. We further refined that population to exclude OIG, Top Secret and Title 13 systems, resulting in a population of 40 systems for our sample selection.

The audit covered the period from October 1, 2025, through July 31, 2026. We performed our audit fieldwork from March to July 2026.

Methodology

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To accomplish our audit objectives, we completed the following procedures:

- Evaluated key components of NARA's information security program and practices, consistent with FISMA and reporting instructions that OMB and DHS issued.
- Focused our testing activities on assessing the maturity of the 20 core and 5 supplemental IG FISMA Reporting Metrics.
- Inspected security policies, procedures, and documentation.
- Performed inquiries and walkthroughs with NARA management and staff.
- Considered guidance contained in OMB's Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, when planning and conducting our work.
- Evaluated select security processes and controls at the program level, as well as for a non-statistical sample of 6 out of 40 information systems in NARA's FISMA reportable system inventory.
- Analyzed the sample of systems selected for testing, including reviewing selected system documentation and other relevant information, as well as testing selected security controls to support the IG FISMA Reporting Metrics.

The *FY 2023-2024 IG FISMA Reporting Metrics* introduced a calculated average scoring model that was continued for the FY 2026 FISMA audit. As part of this approach, IGs must independently calculate the ratings for core and supplemental metrics independently to determine a domain's maturity level and provide data points for the assessed effectiveness of the program and function. To provide IGs with additional flexibility and encourage evaluations that are based on agencies' risk tolerance and threat models, calculated averages were not automatically rounded to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, OMB strongly encouraged IGs to focus on the results of the core metrics, as these tie directly to administration priorities and other high-risk areas. OMB recommended that IGs use the calculated averages of the supplemental metrics as a data point to support their risk-based determination of the overall effectiveness of the program and function.

We used the IG FISMA Reporting Metrics guidance³² to form our conclusions for each CSF domain and function, as well as for the overall agency rating. Specifically, we focused on the calculated average scores of the core metrics. Additionally, we considered other data points,

³² The IG FISMA Reporting Metrics provide the agency IG with the discretion to determine the rating for each of the CSF domains and functions and the overall agency rating based on the consideration of agency-specific factors and weaknesses noted during the FISMA audit. Using this approach, IGs may determine that a particular domain, function area, or agency's information security program is effective at a calculated maturity level lower than level 4.

such as the calculated average scores of the supplemental metrics and progress that NARA has made in addressing outstanding prior-year recommendations, to form our risk-based conclusion.

Our work did not include assessing the sufficiency of internal controls over NARA's information security program or other matters not specifically outlined in this report.

Appendix C: Status of Prior-Year Recommendations

The table below summarizes the status of the recommendations from the prior FISMA audits. At the time of testing and IG FISMA Reporting Metric submission, 15 of 27 recommendations from prior FISMA audits remain open. Additionally, this table maps the prior-year recommendations to the affected IG FISMA Reporting Metric domains.

Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
24-AUD-01 Recommendation 3	Ensure the Information System Security Officers are reviewing system configuration compliance scans monthly as required within NARA's Configuration Compliance Management Standard Operating Procedure.	Closed	Configuration Management
24-AUD-01 Recommendation 9	Finalize and implement system configuration baseline management procedures, which encompass at a minimum, the request, documentation, and approval of deviations from baseline settings for all NARA systems.	Closed	Configuration Management
24-AUD-01 Recommendation 11	Enhance current procedures to ensure that new NARA users who do not complete their initial security awareness training, have their accounts automatically disabled in accordance with timeframes promulgated within the Privacy and Awareness Handbook.	Open	Security Training
24-AUD-01 Recommendation 12	Continue and complete efforts to require PIV authentication for all privileged users, servers and applications, through NARA's Privileged Access Management authentication project and other efforts.	Open	Identity and Access Management
24-AUD-01 Recommendation 13	Enforce mandatory PIV card authentication for all NARANet users, in accordance with OMB requirements.	Closed	Identity and Access Management
24-AUD-01 Recommendation 14	Ensure NARANet user accounts are reviewed and disabled in accordance with NARA's IT policies and requirements.	Open	Identity and Access Management
24-AUD-01 Recommendation 15	Ensure that the Senior Agency Official for Privacy completes Privacy Impact Assessments for all systems which contain Personally Identifiable Information (PII).	Open	Data Protection and Privacy

Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
24-AUD-01 Recommendation 16	The Senior Agency Official for Privacy review and update the NARA 1609 Initial Privacy Reviews and Privacy Impact Assessments privacy policies and procedures to reflect NARA's current processes and controls.	Closed ³³	Data Protection and Privacy
24-AUD-01 Recommendation 17	Implement a process to ensure role-based privacy training is completed by all personnel having responsibility for PII or for activities that involve PII, and content includes, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements.	Closed	Security Training
24-AUD-07 Recommendation 1	Reconcile departure reports received from Human Capital to the asset management inventory system, on a regular basis (e.g., monthly, quarterly, etc.) to ensure updates are being made in a timely manner and are accurate to reflect separated or transferred employees and contractors.	Open	Risk and Asset Management
24-AUD-07 Recommendation 2	Perform a reconciliation of all NARA hardware asset inventories to ensure all data such as assignments and status are accurately and completely stated, investigating any unusual or potentially duplicate entries, and making revisions as needed	Closed	Risk and Asset Management
24-AUD-07 Recommendation 3	Ensure IT policies, procedures, methodologies, and supplements are reviewed and approved in accordance with NARA Directive 111.	Open	Risk and Asset Management
24-AUD-07 Recommendation 5	Implement a process to ensure accounts with access to the Domain Administrators group are appropriately assigned based on job responsibilities. If determined that an account can be configured with more restrictive access, then implement a process to revoke the Domain Administrator group membership and apply the most restrictive access.	Open	Identity and Access Management

³³ This recommendation was closed by NARA OIG prior to the start of the FY 2026 FISMA audit.

Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
24-AUD-07 Recommendation 6	Develop and implement policies and procedures for network user accounts to: ▪ Create unique passwords for each service account. ▪ Maintain a list of commonly used, expected, or compromised passwords. ▪ Update the list on an organization defined timeframe and when organizational passwords are suspected to have been compromised directly or indirectly. ▪ Verify (such as through regular password audits or system configurations), when users create or update passwords, the passwords are not found on the list of commonly used, expected, or compromised passwords.	Open	Configuration Management
24-AUD-07 Recommendation 9	Ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy.	Open	Identity and Access Management
24-AUD-07 Recommendation 12	Ensure password configuration settings for all major information systems are in accordance with NARA IT Security Requirements	Closed	Identity and Access Management
24-AUD-07 Recommendation 13	Ensure the use of shared/group accounts is restricted to only those users with a valid business justification, by enhancing user account review procedures to incorporate reviews of shared/group account membership and reasonableness.	Closed	Identity and Access Management
24-AUD-07 Recommendation 14	Ensure a process is developed, documented, and implemented to change passwords whenever users within shared/group accounts change.	Closed	Identity and Access Management
24-AUD-07 Recommendation 15	Ensure a comprehensive Identity Credential and Access Management policy or strategy, which includes the establishment of related SOPs, identification of stakeholders, communicating relevant goals, task assignments and measure and reporting progress is developed and implemented.	Open	Identity and Access Management
24-AUD-07 Recommendation 16	Implement requirements across all Event Logging maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.	Closed	Incident Response

Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
25-AUD-08 Recommendation 1	Establish and implement guidance for performing NIST CSF 2.0 activities through policies and procedures, including developing current and target cybersecurity profiles that consider anticipated changes in NARA's cybersecurity posture.	Closed	Cybersecurity Governance
25-AUD-08 Recommendation 2	Implement procedures (such as patching and configuration weaknesses) to remediate security vulnerabilities within the defined remediation timeframes specified in the <i>NIST System Security Plan for NARANet General Support System Common Controls</i> and document acceptance of the associated risks, as appropriate.	Open	Configuration Management
25-AUD-08 Recommendation 3	Conduct an assessment to: 1) identify applications running on unsupported platforms and their associated servers; 2) group applications and establish a migration schedule; and 3) migrate applications to vendor-supported platforms. For applications or operating systems that cannot be migrated, document the associated risks and obtain formal acceptance for continued operation.	Open	Configuration Management
25-AUD-08 Recommendation 4	Disable non-essential certificate service endpoints and web enrollment. Additionally, enable features that enhance the protection and handling of credentials when authenticating network connections.	Open	Configuration Management
25-AUD-08 Recommendation 5	Identify all deprecated encryption protocols that NARA uses to secure data in transit and migrate these protocols to vendor-supported protocols.	Open	Data Protection and Privacy
25-AUD-08 Recommendation 6	Implement existing solutions where possible and create a plan to address all exceptions/encryption gaps where NARA does not have a current solution for the encryption of data at rest.	Open	Data Protection and Privacy

Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
25-AUD-08 Recommendation 7	Implement a data loss prevention solution that includes the use or activation of any enhanced data loss prevention features available within NARA's existing tools.	Closed ³⁴	Data Protection and Privacy

³⁴ This recommendation was closed by NARA OIG on August 14, 2026.

Appendix D: Acronyms

Acronym	Definition
C-SCRM	Cybersecurity Supply Chain Risk Management
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSF	Cybersecurity Framework
CPATP	Annual Cybersecurity and Privacy Awareness and Training Program
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
IG	Inspector General
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
SOP	Standard Operating Procedure
SP	Special Publication

Appendix E: Management Comments

Agency management reviewed the draft audit report and provided comments. Agency management stated their general agreement with the findings and recommendations and will provide a Corrective Action Plan by October 30, 2026.

OIG Hotline Contact Information

The OIG Hotline provides a confidential channel for reporting fraud, waste, abuse, and mismanagement to the OIG. In addition to receiving telephone calls at a toll-free Hotline number, we also accept emails through an online referral form.

Visit <https://naraoig.oversight.gov/> for more information, or contact us:

Contact the OIG Hotline

[Online Complaint Form | Office of Inspector General OIG](#)

Contact the OIG by telephone and FAX

Home Telephone: 301-837-3500 (Local) or 1-800-786-2551 (toll-free)

FAX: 301-837-3197

Contractor Self-Reporting Hotline

As required by the Federal Acquisition Regulation, a web-based form allows NARA contractors to notify the OIG, in writing, whenever the contractor has credible evidence a principal, employee, agent, or subcontractor of the contractor has committed a violation of the civil False Claims Act or a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations in connection with the award, performance, or closeout of a contract or any related subcontract. The form can be accessed through the OIG's home page or found directly at [OIG Contractor Reporting Form | Office of Inspector General OIG](#).