NATIONAL ARCHIVES | Inspector General

September 30, 2025

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 2025*
OIG Audit Report No. 25-AUD-08

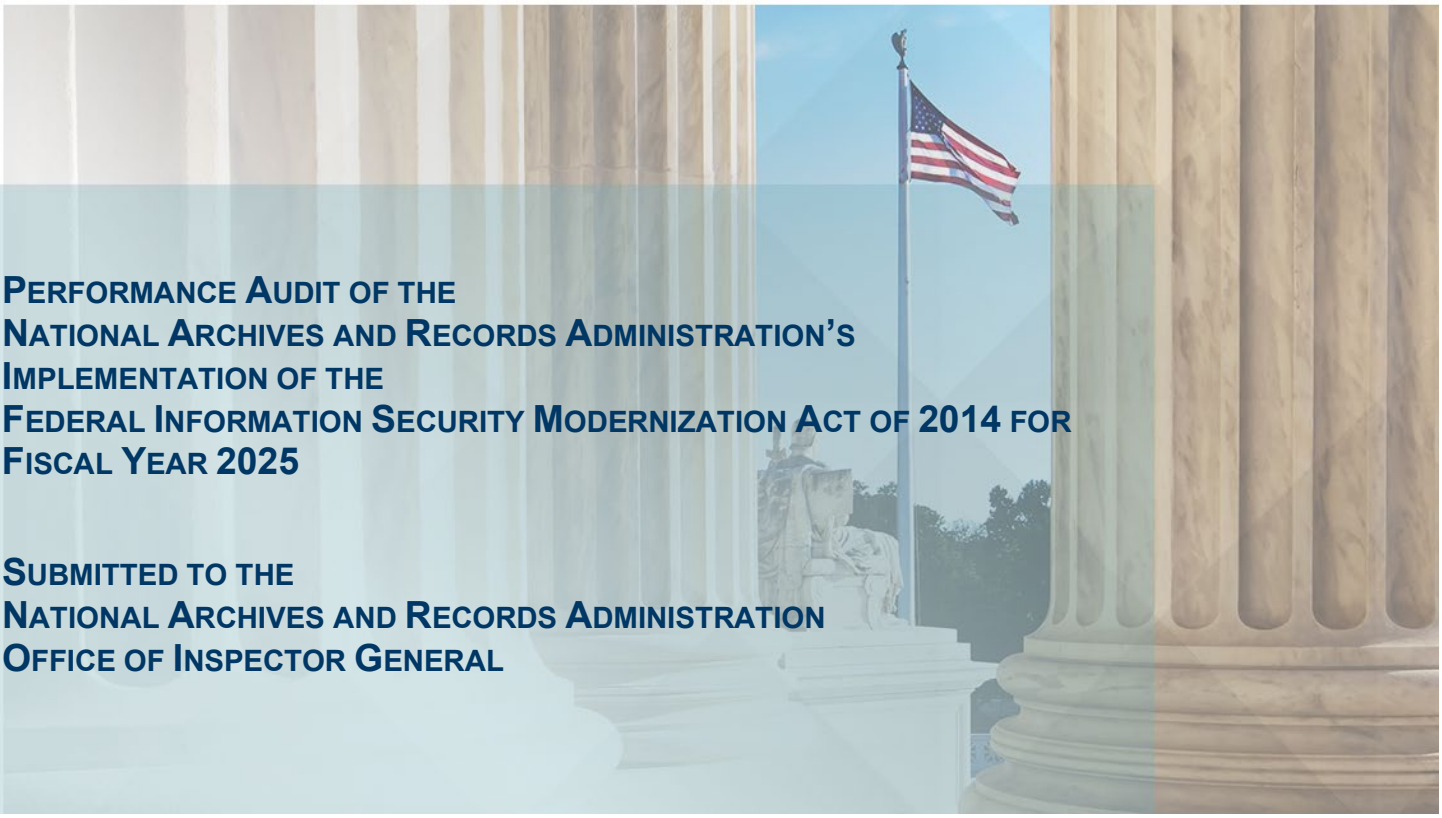
The Office of Inspector General (OIG) contracted with Sikich CPA LLC (Sikich) to conduct an independent audit of the National Archives and Records Administration's (NARA's) information security program and practices in accordance with the Federal Information Security Act of 2014 (FISMA) for fiscal year 2025. Based on this year's FISMA requirements, which included assessing the maturity levels 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*, and three were at Maturity Level 3: *Consistently Implemented*. 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 do not meet the requirements to be considered effective in accordance with FISMA. The report contains seven new recommendations and highlights existing open audit recommendations that are relevant to recurring security control weaknesses.

Sikich is responsible for the attached auditor's report dated September 30, 2025 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.

SIKICH®



PERFORMANCE AUDIT OF THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2025

SUBMITTED TO THE
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

PERFORMANCE AUDIT REPORT

SEPTEMBER 30, 2025

ACCOUNTING TECHNOLOGY ADVISORY

SIKICH®

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

SIKICH.COM

September 30, 2025

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) 2025 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 Inspector General (OIG) engaged Sikich to conduct this performance audit.

The audit covered the period from October 1, 2024, to August 21, 2025. We performed audit fieldwork from March 2025 through August 2025.

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States (2018 Revision, Technical Update April 2021). 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 further 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

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide 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 National Archives and Records Administration (NARA) Office of Inspector General (OIG) 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) annually 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] This memorandum provides reporting guidance for Fiscal Year (FY) 2025 in accordance with 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* (FY 2025 IG FISMA Reporting Metrics).[2]

The FY 2025 IG FISMA Reporting Metrics require us to assess the maturity of six function areas in the agency's information security program and practices. For this year's review, the FY 2025 IG FISMA Reporting Metrics required IGs to assess 20 core[3] and 5 supplemental[4] IG FISMA Reporting Metrics across 6 function areas—Govern,[5] 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 at Level 4:

[1] See OMB Memorandum M-25-04 online: M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf

[2] See the FY 2025 IG FISMA Reporting Metrics online: FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0.

[3] 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 FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0.

[4] Supplemental metrics are assessed at least once every 2 years; they 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 FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0.

[5] In February 2024, NIST published NIST Cybersecurity Framework (CSF) 2.0, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an entity's enterprise risk management strategy. As such, the FY 2025 IG FISMA Reporting Metrics added a new IG FISMA function (Govern) that includes a new domain (Cybersecurity Governance) to align with CSF 2.0.

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

For this audit, we reviewed selected controls outlined in NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020)—which support the FY 2025 IG FISMA Reporting Metrics—for a sample of NARA information systems. The audit covered the period from October 1, 2024, through August 21, 2025. We performed our audit fieldwork from March 2025 to August 2025.

We concluded that NARA's information security program and practices did not meet the requirements to be considered effective in accordance with FISMA. Specifically, NARA's information security program and practices are at Maturity Level 2: *Defined.* As noted above, 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 Cybersecurity Framework (CSF) function and domain in the FY 2025 IG FISMA Reporting Metrics. We determined that three of the CSF function areas for NARA were at Maturity Level 2: *Defined* and three were at Maturity Level 3: *Consistently Implemented.*

Table 1: Maturity Levels for FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Functions[6]	Assessed Maturity Level by Function	Domain	Assessed Maturity Level by Domain
Govern	*Level 2: Defined*	Cybersecurity Governance	Level 2: *Defined* (Not Effective)
		Cybersecurity Supply Chain Risk Management	Level 2: *Defined* (Not Effective)
Identify	*Level 2: Defined*	Risk and Asset Management	Level 2: *Defined* (Not Effective)
Protect	*Level 2: Defined*	Configuration Management	Level 2: *Defined* (Not Effective)
		Identity and Access Management	Level 2: *Defined* (Not Effective)
		Data Protection and Privacy	Level 2: *Defined* (Not Effective)
		Security Training	Level 2: *Defined* (Not Effective)
Detect	*Level 3: Consistently Implemented*	Information Security Continuous Monitoring	Level 3: *Consistently Implemented* (Not Effective)
Respond	Level 3: *Consistently Implemented*	Incident Response	Level 3: *Consistently Implemented* (Not Effective)
Recover	Level 3: *Consistently Implemented*	Contingency Planning	Level 3: *Consistently Implemented* (Not Effective)
Overall	**Level 2: *Defined* (Not Effective)**		

Source: Sikich's assessment of NARA's information security program controls and practices based on the FY 2025 IG FISMA Reporting Metrics.

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

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 and communicated a supply chain risk management strategy and implementation plan.
- Conducted contingency plan testing for the sample of systems in scope.
- Consistently implemented security authorization and assessment processes.

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, Risk and Asset Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, and Incident Response domains of the IG FISMA Reporting Metrics.

In addition, NARA has outstanding open audit recommendations from prior years that significantly impact its ability to improve this year's IG FISMA Reporting Metrics maturity levels. Specifically, at the beginning of the FY 2025 FISMA audit, NARA had 28 open recommendations from prior FISMA audits for 2023[7] and 2024.[8] During our FY 2025 FISMA audit, NARA took corrective actions to address 8[9] of these recommendations, and we consider those recommendations closed. Corrective actions are in progress for the 20 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, the audit team was able to exploit certain vulnerabilities to obtain unauthorized elevated domain account permissions/privileges and access system resources. 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 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 seven new recommendations to assist NARA in strengthening its information security program and practices. In addition, 20 prior-year recommendations remain open.[10]

[7] *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).
[8] *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).
[9] See Appendix C for the status of prior-year recommendations.
[10] See Appendix C for the status of prior-year recommendations.

Table 2: FY 2025 IG FISMA Metric Domains Mapped to New and Prior Year Weaknesses

FY 2025 IG FISMA Metric Domain	Weaknesses Noted
Cybersecurity Governance	NARA has not created guidance for developing and maintaining either a current or a target cybersecurity profile.
Cybersecurity Supply Chain Risk Management	No weaknesses noted.
Risk and Asset Management	NARA has not defined, established, and communicated policies, procedures, roles, and responsibilities for developing and maintaining an inventory of its data and metadata. In addition, prior-year weaknesses related to the review and approval 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, a prior-year weakness related to establishing configuration baseline deviations remained open.
Identity and Access Management	Weaknesses related to inactive accounts persist. In addition, prior-year weaknesses primarily related to continued implementation of multifactor authentication, audit logging, and account management controls remained open.
Data Protection and Privacy	We noted weaknesses in NARA's encryption of sensitive data in transit and at rest, as well as data exfiltration controls. In addition, prior-year weaknesses related to privacy impact assessments and updates to privacy policies and procedures remained open.
Security Training	Prior-year weaknesses related to the completeness of new hire security awareness and role-based privacy training remained open.
Information Security Continuous Monitoring	No weaknesses noted.
Incident Response	Prior-year weaknesses related to the issuance of policies and procedures to support event logging requirements remained open.
Contingency Planning	No weaknesses noted.

Source: Sikich's assessment of NARA's information security program controls and practices based on the FY 2025 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 objective, scope, and methodology of the audit. **Appendix C** provides the current status of prior-year FISMA report recommendations. **Appendix D** provides a listing of acronyms used throughout this report. **Appendix E** contains management's comments on the report.

II. AUDIT RESULTS

The following section of the report describes the key controls underlying each function and domain and our assessment of NARA's maturity and 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 CSF 2.0.

Security 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 its 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* and identified the following weakness:

NARA has not developed or implemented NIST CSF 2.0[11] through its policies and procedures. Specifically, NARA did not document guidance for performing CFS 2.0 activities, such as developing and maintaining both current and target cybersecurity profiles.[12]

NARA management stated that developing unique CSF 2.0 organizational risk profiles has not been a priority for NARA, as NIST only finalized and released CSF 2.0 last year.

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)[13] developed by NIST, or any successor document, to manage the agency's cybersecurity risk.*

The Government Accountability Office's *Standards for Internal Control in the Federal Government* (September 2014), GAO-14-704G, *Principle 12 – Implement Control Activities*, states:

> *12.01 Management should implement control activities through policies*.
>
> *12.02 Management documents in policies the internal control responsibilities of the organization.*

[11] See NIST CSF 2.0 online: The NIST Cybersecurity Framework (CSF) 2.0.
[12] NIST CSF 2.0 (February 26, 2024) provides guidance to assist with managing cybersecurity risks. Section 3.1 offers guidance on the use of cybersecurity profiles to understand, tailor, assess, prioritize, and communicate cybersecurity objectives. A CSF organizational profile describes an organization's current and/or target cybersecurity posture in terms of the CSF core's outcomes. The CSF core is a taxonomy of high-level cybersecurity outcomes that can help organizations manage their cybersecurity risks. The CSF core components are a hierarchy of functions, categories, and subcategories that detail each outcome.
[13] 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.

The absence of current and target CSF profiles increases the risk that NARA might not appropriately consider or address cybersecurity risks. It may also increase the risk of issues such as, but not limited to, breaches, system interruptions, and exploited vulnerabilities.

Recommendations:

We recommend that the NARA Chief Information Officer take the following action related to the weakness noted for the Cybersecurity Governance domain:

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.

Metric Domain: Cybersecurity Supply Chain Risk Management

An agency with an effective cybersecurity supply chain risk management 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 cybersecurity supply chain risk management domain is Level 2*: Defined*. Although NARA has developed and communicated a supply chain risk management strategy, it is still in the process of implementing key components. These components include tasks such as rolling out vendor software self-attestations, finalizing contractual clauses related to supply chain risk management, and completing various tasks outlined in NARA's implementation plan to bring NARA into compliance with OMB Memorandum M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (June 9, 2023).

Recommendations:

We are not making any recommendations for the Cybersecurity Supply Chain Risk Management domain.

Security Function: Identify

The objective of the Identify function is to develop an understanding of the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks to enable the organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under the Govern function. 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, software assets, and data management; 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 three open prior-year recommendations in the Risk and Asset Management domain.[14] 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.

In addition, NARA has not defined and established policies, procedures, roles, and responsibilities for developing and maintaining an inventory of its data and corresponding metadata and communicated these items across the organization.[15] This increases the risk that NARA will be unable to properly account for and secure its sensitive data. Because the NARA OIG identified data inventory weaknesses in OIG Audit Report 24-AUD-09, *Audit of NARA's Cloud Computing Services* (September 30, 2024),[16] we are not making a new recommendation related to data inventory in this report.

Recommendations:

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.[17]

Security 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 2025, 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

[14] Recommendations 1, 2, 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.
[15] OMB Memorandum M-25-05, *Phase-2 Implementation of the Foundations for Evidence Based Policymaking Act of 2018: Open Government Data Access and Management Guidance* defines metadata as "structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection, and other descriptions."
[16] Recommendations 1 and 2 (OIG Audit Report No. 24-AUD-09, September 30, 2024).
[17] Prior FISMA open recommendations related to the Risk and Asset Management domain include Recommendations 1, 2, and 3 (OIG Audit Report No. 24-AUD-07, September 27, 2024). See Appendix C for additional information regarding these prior-year recommendations. Additionally, Recommendations 1 and 2 (OIG Audit Report No. 24-AUD-09, September 30, 2024). We are not repeating these recommendations within this report.

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 domain[18] that relate to improving its vulnerability management program and establishing baseline configuration deviations.

In addition, the independent vulnerability assessment and penetration test that we performed during the FY 2025 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, as discussed below.

Vulnerability Management Program and Processes

Our independent vulnerability assessments of NARA's network and a sample of in-scope systems identified critical and high-risk vulnerabilities related to patch management, configuration management, and unsupported software that may enable malicious actors to gain unauthorized access to mission-critical systems and data. Further, NARA did not timely remediate vulnerabilities that are included in the Cybersecurity & Infrastructure Security Agency's (CISA's)[19] Known Exploitable Vulnerability catalog.[20]

In addition, we performed a penetration test and identified misconfigured certificate services,[21] weaknesses related to weak and reused passwords, and accounts with excessive administrative access. 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.

NARA is in the process of implementing corrective actions for prior-year recommendations related to patch management, configuration weaknesses, 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 service 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, and web enrollment services. Furthermore, we were able to authenticate with accounts in the domain administrator group because NARA had not configured them to require multifactor authentication.

[18] Recommendations 3 and 9 (OIG Audit Report No. 24-AUD-01, October 24, 2023) and Recommendations 5 and 6 (OIG Audit Report No. OIG-24-AUD-07, September 27, 2024). See Appendix C for additional information regarding these prior-year recommendations.
[19] CISA, a component of DHS, is responsible for cybersecurity and infrastructure protection for all levels of government.
[20] To help organizations better manage vulnerabilities and keep pace with threat activity, CISA maintains the authoritative source of vulnerabilities that have been exploited, along with the date by which agencies are required to remediate each vulnerability. See CISA Known Exploited Vulnerabilities Catalog for more details.
[21] As an example, Active Directory Certificate Services is a Windows Server role for issuing and managing public key infrastructure certificates used in secure communications and authentication protocols. See What is Active Directory Certificate Services for more details.

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

> *(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.*

In addition, CISA's Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, states that agencies are required to remediate each vulnerability in accordance with the timelines set forth in the CISA-managed vulnerability catalog. The catalog lists exploited vulnerabilities that carry significant risk to the federal enterprise and requires agencies to remediate vulnerabilities within 6 months for vulnerabilities with a Common Vulnerabilities and Exposures (CVE)[22] ID assigned prior to 2021 and within 2 weeks for all other vulnerabilities. These default timelines may be adjusted in the case of grave risk to the federal enterprise.

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 the following actions related to the weaknesses identified for the Configuration Management domain, in addition to addressing open prior-year recommendations:[23]

2. Implement procedures (such as patching and configuration weaknesses) to remediate security vulnerabilities within the defined remediation timeframes specified in the *NIST System Security Plan for NARANet General Support System Common Controls* and document acceptance of the associated risks, as appropriate.

3. Conduct an assessment to: 1) identity 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.

[22] CVE is a list of all publicly known vulnerabilities that include the CVE ID.
[23] Open prior-year FISMA recommendations related to the findings noted within the Configuration Management domain include Recommendation 6 (OIG Audit Report No. 24-AUD-07, September 27, 2024) and Recommendations 3 and 9 (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.

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.

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 has opportunities to improve its identity and access management program by implementing the eight open prior-year recommendations in this area.[24] These recommendations primarily relate to the continued implementation of multifactor authentication, audit logging, 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

During FY 2025, we identified continued weaknesses in account management for inactive user accounts, as follows:

- Based on a review of NARANet user accounts, we found that 406 of the 3,890 user accounts had not logged in for more than 90 days, and NARA had not disabled the accounts in accordance with its policy.
- Based on a comparison of NARANet user accounts to employees who separated from NARA between October 1, 2024, and March 31, 2025, we found that NARA had not disabled the NARANet accounts for 20 of the individuals who had separated from NARA.

NARA's Office of Information Services acknowledges that there are gaps in its operations team's understanding of all of NARA's intricate scripts and their interactions, which has led to an unintended re-enabling of accounts that NARA had previously disabled due to inactivity, including accounts of separated users. NARA management stated that they are reviewing and assessing all scripts and configurations related to account management to identify and rectify these underlying issues. In addition, NARA has not corrected deficiencies from prior years related to periodic reviews and automated disabling of user system accounts for all systems and NARANet user accounts.

NARA User Account and Privileged User Account Management Standard Operating Procedure (SOP), Version 8.0 (December 31, 2024), states, "All accounts will be disabled after 60 days and de-provisioned after 90 days."

[24] Recommendations 9, 12, 13, 14, and 15 (OIG Audit Report No. 24-AUD-07, September 27, 2024) and Recommendations 12, 13, 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.

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

> *When a user separates or terminates from NARA and no longer needs access to NARANet, the account is disabled and scheduled for de-provisioning. If the account disablement decision changes, a ten business day window is provided.*
>
> *When an account has been inactive for over 30 days, the OIG will receive an email notification 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 user accounts in a timely manner when it no longer needs them, there is an increased risk that unauthorized individuals may access these accounts.

Recommendations:

We recommend that the NARA Chief Information Officer take actions to address open prior-year recommendations related to the Identity and Access Management domain.[25]

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; is able to assess its security and privacy controls, as well as its breach response capacities; 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 two open prior-year recommendations in this area related to completing privacy impact assessments and updating privacy policies and procedures.[26] In addition, during the current year's audit, we noted the following weaknesses, as detailed below.

We noted that NARA's implementation of data protection and privacy controls was not effective across the entire organization with regard to the encryption of sensitive data and data exfiltration. Specifically, we noted the following:

- When securing data in transit, NARA is using encryption protocols that the vendor has deprecated[27] and are considered outdated and insecure. Specifically, the documentation that NARA provided shows that NARA is still using versions of its encryption protocols (running on a total of 321 devices) that the vendor has deprecated and that are therefore vulnerable to security flaws and connection issues.

[25] Open prior-year FISMA recommendations related to the findings noted within the Identity and Access Management domain include Recommendations 9, 12, 13, 14, and 15 (OIG Audit Report No. 24-AUD-07, September 27, 2024) and Recommendations 12, 13, 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.

[26] Recommendations 15 and 16 (OIG Audit Report No. OIG-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] As defined by NIST, the term deprecated means that the algorithm and key length may be used, but the user must accept some security risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection. Deprecated - Glossary | CSRC

- The NARA Chief Information Officer 2024 FISMA Quarter 4/Annual report stated that, as of September 30, 2024, not all NARA systems that stored sensitive data were encrypting that data when it was at rest. Specifically, only 34 of the 46 systems (approximately 74 percent) encrypted sensitive data at rest.
- NARA has not fully implemented Data Loss Prevention (DLP) solutions to ensure comprehensive data protection agency-wide. Although NARA has taken steps to strengthen its data protection—such as piloting solutions, evaluating DLP solutions across other environments, and planning to form a working group to develop a comprehensive data protection strategy— these initiatives are still in progress, and NARA has yet to realize a fully implemented, agency-wide data protection framework.

With regard to the devices with outdated encryption protocols for securing data in transit, NARA's IT Operations Team determined that approximately 75 percent of the devices were printers that require security enhancements, and another 24 percent were devices that reside on vendor-unsupported servers or network devices that are scheduled for decommissioning, upgrade, or replacement. Only 1 percent of the devices were application-specific servers for which NARA (and the contractors who support the servers) would need to disable legacy encryption protocols. In addition, NARA has performed reviews of its systems to identify gaps where it is not currently encrypting sensitive data.[28]

Furthermore, although NARA has not fully developed a comprehensive, agency-wide DLP solution, it stated that it has several efforts ongoing in this area, including piloting data protection tools, exploring DLP solutions, planning to establish a working group, and developing an inventory and evaluation of databases to account for personally identifiable information (PII) protection and database backup and recovery policies, as part of an overall DLP strategy.

NARA IT Security Requirements, version 7.4 (November 8, 2023), *SC-7(10) Prevent Exfiltration,* states:

> *For data deemed by the NARA System Owner to require this additional integrity protection, the NARA Office of Information Services (I) shall:*
>
> *a) Prevent the exfiltration of information*

NARA IT Security Requirements, version 7.4 (November 8, 2023), *AC-17(2) Protection of Confidentiality and Integrity using Encryption,* states:

> *For data requiring moderate or high confidentiality, the system shall implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.*

Without implementing data encryption and data exfiltration mechanisms, there is an increased risk of unauthorized disclosure or modification of sensitive data. Additionally, continuing to secure data in transit by using encryption protocols that the vendors have deprecated and that are considered outdated and insecure could result in connectivity issues and security flaws.

[28] NARA indicated they have identified those systems where encryption gaps remain and expect to identify solutions to address those gaps. The implementation of encryption for data at rest on those systems has a target resolution date of December 31, 2025.

Recommendations:

We recommend that the NARA Chief Information Officer take the following actions related to the weaknesses identified for the Data Protection and Privacy domain, in addition to addressing open prior-year recommendations:[29]

5. Identify all deprecated encryption protocols that NARA uses to secure data in transit and migrate these protocols to vendor-supported protocols.

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.

7. Implement a DLP solution that includes the use or activation of any enhanced DLP features available within NARA's existing tools.

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.

We determined that the maturity level for NARA's Security Training domain is Level 2: *Defined*. NARA has two open prior-year recommendations in this area that are 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.[30]
- Implementing a process to ensure that all personnel who are responsible for PII—or for activities that involve PII—complete role-based privacy training.[31]

Although NARA described its information security workforce program in response to the annual CIO FISMA Metrics and conducts a verbal assessment prior to assigning and identifying specific training needs, these actions—combined with the two open prior-year recommendations—were not sufficient for NARA to advance to the next maturity level.

Recommendations:

We recommend that the NARA Chief Information Officer take actions to address open prior-year recommendations related to the weaknesses noted for the Security and Training domain.[32]

[29] Open prior-year FISMA recommendations related to the Data Protection and Privacy domain include Recommendations 15 and 16 (OIG Audit Report No. OIG-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.
[30] Recommendation 11 (OIG Audit Report No. 24-AUD-01, October 24, 2023). We are not repeating this recommendation within this report.
[31] Recommendation 17 (OIG Audit Report No. 24-AUD-01, October 24, 2023). We are not repeating this recommendation within this report.
[32] Prior FISMA open recommendations related to the Security Training domain include Recommendations 11 and 17 (OIG Audit Report No. 24-AUD-01, October 24, 2023). See Appendix C for additional information regarding the prior-year recommendations. We are not repeating this recommendation within this report.

Security 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 3: *Consistently Implemented.*

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 for NARA's Information Security Continuous Monitoring domain is Level 3: *Consistently Implemented.* We noted that there are no open prior-year recommendations for this domain.

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 the Security Operations Center as a Service through the Department of Justice's Cybersecurity Shared Services to provide additional real-time incident response capabilities. NARA also indicated that they utilize various automated tools to support their assessment activities under the Security Assessment and Authorization process. However, NARA should continue to enhance its capabilities to automate and integrate these functions in near real-time with its Governance, Risk and Compliance tool. As a result, NARA has not yet achieved a higher maturity level for the Information Security Continuous Monitoring domain.

Recommendations:

We are not making any recommendations for the Information Security Continuous Monitoring domain.

Security Function: Respond

The objective of the Respond function is to ensure that organizations take action when they detect a cybersecurity incident. 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.
- 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 demonstrated strengths in this area by implementing incident response policies and procedures for identifying, managing, and responding to cybersecurity-related incidents. However, NARA has one open prior-year recommendation in this domain[33] related to implementing the requirements for event logging identified in OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021).[34]

Recommendations:

We recommend that the NARA Chief Information Officer take action to address the open prior-year recommendation related to the weaknesses noted for the Incident Response domain.[35]

Security 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 for 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 (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 has employed automated mechanisms to test contingency plans more

[33] Recommendation 16 (OIG Audit Report No. 24-AUD-07, September 27, 2024). See Appendix C for additional information regarding the prior-year recommendations. We are not repeating this recommendation within this report.
[34] Refer to OMB Memorandum M-21-31.
[35] The open prior-year FISMA recommendation related to the Incident Response domain is Recommendation 16 (OIG Audit Report No. 24-AUD-07, September 27, 2024). See Appendix C for additional information regarding the prior-year recommendations. We are not repeating this recommendation within this report.

thoroughly and effectively. As a result, NARA has not yet achieved a higher maturity level for the Contingency Planning domain.

Recommendations:

We are not making any recommendations 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 agency-wide 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 to 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 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 annually 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*. This memorandum provides reporting guidance and deadlines for FY 2025 in accordance with 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.

One of the goals of the annual FISMA evaluations is to assess agencies' progress toward achieving objectives that strengthen federal cybersecurity. The FY 2025 IG FISMA Reporting Metrics were updated to reflect recent developments:

- NIST published CSF 2.0 in February 2024, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into enterprise risk management strategy. The FY 2025 IG FISMA Reporting Metrics therefore added a new IG FISMA function (Govern) that includes a new domain (Cybersecurity Governance), to align with NIST CSF 2.0.
- To align with CSF 2.0, the Supply Chain Risk Management domain moved from the Identify function to the Govern function, to better reflect agency oversight of supply chain risk.
- The FY 2025 IG FISMA Reporting Metrics introduced a new domain, Risk and Asset Management, in the Identify function to group metrics on system inventory and hardware, software, and data management.
- Five supplemental metrics are in scope for the FY 2025 IG FISMA evaluation, including two new supplemental metrics that are focused on system-level risk management practices critical to achieving Zero Trust Architecture objectives.

- The FY 2025 IG FISMA Reporting Metrics revised the core metric on information system-level risk management to focus on the maturity of agencies' implementation of the NIST Risk Management Framework.

As highlighted in **Table 3**, the FY 2025 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 2.0: Govern, Identify, Protect, Detect, Respond, and Recover.

Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Function Area	Function Area Objective	Domain(s)
Govern	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	Cybersecurity Governance and Cybersecurity Supply Chain Risk Management
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	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 2.0 and the FY 2025 IG FISMA Reporting Metrics.

The foundational levels of the maturity model in the IG FISMA Reporting Metrics focus on the development of 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 Level 4: *Managed and Measurable* or higher.

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, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2025 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 2025. The scope also included assessing selected controls from NIST SP 800-53, Revision 5—which support the FY 2025 IG FISMA Reporting Metrics—for a sample of 6 systems from a total population of 49 NARA FISMA reportable systems[36] as of March 21, 2025 (**Table 5**).

Table 5: Description of System Selected for Testing

System Name	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.
Digital Delivery Platform (DDP)	Supports records centers program scanning operations.
Electronic Records Administration – Executive Office of the President (ERA EOP)	Electronic records preservation and search & access system which contain Presidential Records Act and Federal Records Act electronic records.
G-Suite Enterprise (G Suite)	NARA's email calendaring and collaboration suite system.

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 IG FISMA Reporting 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. Refer to **Appendix C** for the status of prior-year recommendations.

[36] NARA's population of FISMA-reportable systems as of March 21, 2025, included 53 systems that NARA identified as a "Major Application" or "General Support System." We refined this population to exclude OIG and Title 13 systems, resulting in a population of 49 systems for our sample selection. We selected the six systems in coordination with the OIG.

The audit covered the period from October 1, 2024, through August 21, 2025. We performed audit fieldwork from March 2025 to August 2025.

Methodology

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States (2018 Revision, Technical Update April 2021). 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 objective, we completed the following procedures:

- Evaluated key components of NARA's information security program and practices, consistent with FISMA and with reporting instructions that OMB and DHS issued for FY 2025.
- Focused testing activities on assessing the maturity of the 20 core and 5 supplemental IG FISMA Reporting Metrics.
- Inspected security policies, procedures, and documentation.
- Made inquiries of 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 of the 49 information systems in NARA's system inventory.
- Analyzed the sample of systems selected for testing, including reviewing selected system documentation and other relevant information, as well as tested selected security controls to support the IG FISMA Reporting Metrics.
- Reviewed the status of prior-year FISMA recommendations. See **Appendix C** for the status of the prior-year recommendations.

The *FY 2023-2024 IG FISMA Reporting Metrics* introduced a calculated average scoring model that was continued for the FY 2025 FISMA audit. As part of this approach, IGs must average the ratings for core and supplemental IG FISMA Reporting 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, the IG FISMA Reporting Metrics do not automatically round calculated averages 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 IG FISMA Reporting Metrics, as these tie directly to administration priorities and other high-risk areas. OMB recommended that IGs use the calculated averages of the supplemental IG FISMA Reporting Metrics as a data point to support their risk-based determination of the overall effectiveness of the program and function.

We used the FY 2025 IG FISMA Reporting Metrics guidance[37] 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 IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average scores of the supplemental IG FISMA Reporting 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 and other matters not specifically outlined in this report.

[37] The FY 2025 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.

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, 20 of the 28 recommendations from prior FISMA audits remain open. Additionally, this table maps the prior-year recommendation to the affected IG FISMA Reporting Metric domains.

OIG Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
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.	Open	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 4	Develop and communicate an organization wide Supply Chain Risk Management strategy and implementation plan to guide and govern supply chain risks.	Closed[38]	Cybersecurity Supply Chain Risk Management

[38] The recommendation was closed by the NARA OIG prior to the start of the FY 2025 FISMA audit.

OIG Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
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	Configuration Management
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

OIG Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
24-AUD-07 Recommendation 7	Assess applications residing on unsupported platforms to identify a list of applications, all servers associated to each application, and the grouping and schedule of applications to be migrated, with the resulting migration of applications to vendor-supported platforms.	Closed	Configuration Management
24-AUD-07 Recommendation 8	Implement the following: • Complete efforts to implement the Security Information and Event Management product. • Develop and implement processes and procedures to monitor and at least weekly review user activity and audit logs (in accordance with NARA IT Security Requirements), on systems that may indicate potential security violations. • Ensure the procurement of new IT system hardware and software, which provides user authentication, includes a minimum set of audit logging.	Closed[39]	Incident Response
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

[39] The recommendation was closed by the NARA OIG prior to the start of the FY 2025 FISMA audit.

OIG Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
O24-AUD-07 Recommendation 10	Ensure audit logging is enabled for each major information system.	Closed	Identity and Access Management
24-AUD-07 Recommendation 11	Ensure periodic reviews of generated audit logs are performed for each major information system.	Closed	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.	Open	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.	Open	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.	Open	Identity and Access Management
24-AUD-07 Recommendation 15	Ensure a comprehensive Identity Credential and Access Management (ICAM) 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	Open	Incident Response

OIG Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
	ensure events are logged and tracked in accordance with OMB M-21-31.		
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 SOP.	Open	Configuration Management
24-AUD-01 Recommendation 5	Implement improved processes to remediate security deficiencies on NARA's network infrastructure, to include enhancing its patch and vulnerability management program to address security deficiencies identified during our assessments of NARA's applications and network infrastructure.	Closed	Configuration Management
24-AUD-01 Recommendation 7	Document and implement a process to track and remediate persistent configuration vulnerabilities or document acceptance of the associated risks.	Closed	Configuration Management
24-AUD-01 Recommendation 8	Ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported.	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	Open	Configuration Management

OIG Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
	baseline settings for all NARA systems.		
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 Personal Identifier Verification (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.	Open	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 (SAOP) completes Privacy Impact Assessments for all systems which contain PII.	Open	Data Protection and Privacy
24-AUD-01 Recommendation 16	The SAOP will review and update NARA's 1609 Initial Privacy Reviews and Privacy Impact Assessments privacy policies and	Open	Data Protection and Privacy

OIG Report No. Recommendation No.	Recommendation	Status	Affected IG FISMA Reporting Metric Domains
	procedures to reflect NARA's current processes and controls.		
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.	Open	Security Training

APPENDIX D: ACRONYMS

Acronym	Definition
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity and Infrastructure Security Agency
CSF	Cybersecurity Framework
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DLP	Data Loss Prevention
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ICAM	Identity Credential and Access Management
IG	Inspector General
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identify Verification
SAOP	Senior Agency Official for Privacy
SOP	Standard Operating Procedure
SP	Special Publication

APPENDIX E: MANAGEMENT COMMENTS

Agency management stated their general agreement with the findings and recommendations and opted not to provide formal comments for inclusion in this report.

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