




Inspector General

September 27, 2024

TO: Dr. Colleen Shogan  
Archivist of the United States

FROM: Dr. Brett M. Baker   
Inspector General

SUBJECT: *National Archives and Records Administration's Fiscal Year 2024 Federal Information Security Modernization Act of 2014 Audit*  
OIG Audit Report No. 24-AUD-07

The Office of Inspector General (OIG) contracted with Sikich to conduct an independent audit on the National Archives and Records Administration's (NARA) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year 2024. Based upon the audit of NARA's information security program, including its compliance with FISMA and OMB/DHS requirements in the function areas, Sikich concluded that NARA's information security program was "Not Effective." In addition, NARA's overall maturity level remained at a level of "Consistently Implemented." The report contains three new recommendations and 13 repeat recommendations from prior year FISMA audits (which have missed their targeted completion dates) to help NARA address challenges in its development of a mature and effective information security program. Agency staff indicated they had no comments for inclusion in this report.

Sikich is responsible for the attached auditor's report dated September 27, 2024 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 Auditing 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 letter. As with all OIG products, we determine what information is publicly posted on our website from the attached report. Consistent with our responsibility under the *Inspector General Act, as amended*, we will provide copies of our report to congressional committees with oversight responsibility over NARA.

We appreciate the cooperation and assistance NARA extended to Sikich and my staff during the audit. Please contact me with any questions.

Attachment

cc: Merrily Harris, Executive Secretariat  
William Bosanko, Deputy Archivist  
Jay Trainer, Acting Chief Operating Officer  
Meghan Guthorn, Deputy Chief Operating Officer  
Colleen Murphy, Acting Chief of Management and Administration and Chief Financial Officer  
Sheena Burrell, Chief Information Officer  
Nicole Willis, Deputy Chief Information Officer  
Kimm Richards, Accountability  
Carol Seubert, Senior Auditor  
United States Senate Homeland Security and Governmental Affairs Committee  
United States House of Representatives Committee on Oversight and Reform



**PERFORMANCE AUDIT OF THE  
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION  
IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY  
MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2024**

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

**PERFORMANCE AUDIT REPORT**

**SEPTEMBER 27, 2024**



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

**SIKICH.COM**

September 27, 2024

Dr. Brett Baker  
Inspector General  
Office of Inspector General  
National Archives and Records Administration

Dear Dr. Baker:

Sikich CPA LLC (Sikich)<sup>1</sup> is pleased to submit the attached report detailing the results of our performance audit of the National Archives and Records Administration (NARA's) information security program, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), for Fiscal Year 2024. FISMA requires federal agencies, including NARA, to perform an annual independent evaluation of their information security program. FISMA states that the evaluation is to be performed by the agency Inspector General (IG) or by an independent external auditor as determined by the IG. The NARA Office of Inspector General engaged Sikich to conduct this performance audit. The audit covered the period October 1, 2023, through July 30, 2024. We performed audit fieldwork from November 2023 to July 2024.

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). These 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.

*Sikich CPA LLC*

Alexandria, VA

---

<sup>1</sup> Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP's federal practice, including its work for the National Archives and Records Administration Office of Inspector General.

**TABLE OF CONTENTS**

<b>I.</b>	<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>II.</b>	<b>SUMMARY OF RESULTS .....</b>	<b>2</b>
<b>III.</b>	<b>AUDIT RESULTS.....</b>	<b>5</b>
	SECURITY FUNCTION: IDENTIFY.....	5
	SECURITY FUNCTION: PROTECT.....	8
	SECURITY FUNCTION: DETECT.....	13
	SECURITY FUNCTION: RESPOND .....	14
	SECURITY FUNCTION: RECOVER .....	15
	<b>APPENDIX A: BACKGROUND.....</b>	<b>17</b>
	<b>APPENDIX B: OBJECTIVE, SCOPE, AND METHODOLOGY.....</b>	<b>19</b>
	<b>APPENDIX C: STATUS OF PRIOR FISMA REPORT RECOMMENDATIONS .....</b>	<b>21</b>
	<b>APPENDIX D: ACRONYMS .....</b>	<b>25</b>
	<b>APPENDIX E: AGENCY COMMENTS .....</b>	<b>26</b>
	<b>APPENDIX F: REPORT DISTRIBUTION LIST.....</b>	<b>27</b>
	<b>OIG HOTLINE INFORMATION.....</b>	<b>28</b>

## 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 (FIPS) to establish agency baseline security requirements.

The National Archives and Records Administration (NARA's) Office of Inspector General (OIG) engaged Sikich CPA LLC (Sikich)<sup>2</sup> 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 assess the effectiveness of NARA's information security program and practices in accordance with FISMA and applicable instructions from OMB and the Department of Homeland Security (DHS) IG FISMA Reporting Metrics.

OMB and DHS annually provide federal agencies and IGs with instructions for preparing FISMA reports. On December 4, 2023, the OMB issued Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*.<sup>3</sup> This memorandum describes the methodology for conducting FISMA audits and the process for federal agencies to report to OMB and, where applicable, DHS. According to that memorandum, each year IGs are required to complete the IG FISMA Reporting Metrics<sup>4</sup> to independently assess their agency's information security program.

For this year's review, IGs were required to assess 20 core<sup>5</sup> and 17 supplemental<sup>6</sup> IG FISMA Reporting Metrics across five security function areas—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: *Managed and Measurable*, or above. 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*

---

<sup>2</sup> Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP's federal practice, including its work for NARA's OIG.

<sup>3</sup> See OMB M-24-04 at <https://www.whitehouse.gov/wp-content/uploads/2023/12/M-24-04-FY24-FISMA-Guidance.pdf>

<sup>4</sup> See the Fiscal Year (FY) 2023 – 2024 IG FISMA Reporting Metrics at [https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1\\_0.pdf](https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1_0.pdf). We provided the NARA OIG with our responses to the FY 2024 IG FISMA Reporting Metrics as a separate deliverable under the contract for this audit.

<sup>5</sup> Core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness.

<sup>6</sup> 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 security program effectiveness.

(September 2020), supporting Fiscal Year (FY) 2024 IG FISMA reporting metrics, for a sample of NARA information systems. The audit covered the period October 1, 2023, through July 30, 2024. We performed our audit fieldwork from November 2023 to July 2024.

## II. SUMMARY OF RESULTS

Based on our audit of NARA's information security program and practices, including its compliance with FISMA, OMB, and DHS requirements in the function areas, we concluded that NARA's information security program and practices was "Not Effective." Specifically, NARA achieved an overall maturity level of Level 3: *Consistently Implemented*. We noted that one functional area achieved a maturity level of Level 1: *Ad Hoc*, one functional area achieved a maturity level of Level 2: *Defined* and three functional areas achieved a maturity level of Level 3: *Consistently Implemented* for an overall maturity level of Level 3: *Consistently Implemented* for the security program. **Table 1** below summarizes the overall maturity levels for each security function and domain in the FY 2024 IG FISMA Reporting Metrics.

**Table 1: Maturity Levels for FY 2024 IG FISMA Reporting Metrics**

Cybersecurity Framework Security Functions <sup>7</sup>	Maturity Level by Function	Domain	Maturity Level by Domain
Identify	Level 1: Ad Hoc	Risk Management	Level 2: <i>Defined</i> (Not Effective)
Identify	Level 1: Ad Hoc	Supply Chain Risk Management (SCRM)	Level 1: <i>Ad-Hoc</i> (Not Effective)
Protect	Level 2: <i>Defined</i>	Configuration Management	Level 2: <i>Defined</i> (Not Effective)
Protect	Level 2: <i>Defined</i>	Identity and Access Management	Level 2: <i>Defined</i> (Not Effective)
Protect	Level 2: <i>Defined</i>	Data Protection and Privacy	Level 2: <i>Defined</i> (Not Effective)
Protect	Level 2: <i>Defined</i>	Security Training	Level 2: <i>Defined</i> (Not Effective)
Detect	Level 3: <i>Consistently Implemented</i> (Not Effective)	Information Security Continuous Monitoring (ISCM)	Level 3: <i>Consistently Implemented</i> (Not Effective)
Respond	Level 3: <i>Consistently Implemented</i> (Not Effective)	Incident Response	Level 3: <i>Consistently Implemented</i> (Not Effective)
Recover	Level 3: <i>Consistently Implemented</i> (Not Effective)	Contingency Planning	Level 3: <i>Consistently Implemented</i> (Not Effective)
Overall	Level 3: <i>Consistently Implemented</i> (Not Effective)		

Source: Sikich's assessment of NARA's information security program controls and practices based on the FY 2024 IG FISMA Reporting Metrics.

We determined that NARA established a number of 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:

- Developed configuration management plans and processes for NARA systems, even those not under enterprise configuration management program management control.
- Improved controls over the disabling of user accounts upon separation of employment.
- Strengthened security assessment and authorization processes.

<sup>7</sup> See Table 3 and Table 4 in Appendix A for definitions and explanations of the Cybersecurity Framework security functions and FISMA metric domains and maturity levels, respectively.



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 towards a "Managed and Measurable" maturity level, NARA will need to address the new and repeat weaknesses in its security program related to the Risk Management, SCRM, Configuration Management, Identity and Access Management, Information Security Continuous Monitoring, Data Protection and Privacy, Security Training, and Incident Response domains of the IG FISMA Reporting Metrics.

Additionally, outstanding prior-year recommendations continue to significantly impact NARA's ability to improve its IG FISMA Reporting Metrics maturity levels. Specifically, at the beginning of the FY 2024 FISMA audit, NARA had 31 open recommendations from prior FISMA audits dating from 2021 through 2023. During our 2024 FISMA audit, we found that NARA took corrective actions to address five of the recommendations, and we consider those recommendations closed. Corrective actions are in progress for the other 26 open recommendations.<sup>8</sup>

Some of the recurring security weaknesses present a significant risk to NARA, including unsupported software, missing patches, and configuration weaknesses. These weaknesses may allow unauthorized access into mission-critical systems and data. Many of these vulnerabilities have existed since they were publicly known prior to 2023. As a result, the assessment team was able to exploit certain vulnerabilities to obtain unauthorized elevated user permissions/privileges and access system resources.

At present, the new and repeat weaknesses that we identified (as summarized in **Table 2**) leave NARA operations and assets at risk of unauthorized access, misuse, and disruption. We made three new recommendations to help NARA address challenges in its development of a mature and effective information security program and practices. In addition, of the 26<sup>9</sup> prior year recommendations that remain open, we included within the body of the report, 13 prior-year recommendations which have missed target completion dates.

**Table 2: FY 2024 IG FISMA Metric Domains Mapped to Weaknesses Noted in 2024 NARA FISMA Audit**

FY 2024 IG FISMA Metric Domains	Weaknesses Noted
Risk Management	NARA does not maintain a complete and accurate inventory of its hardware assets. In addition, a prior year weakness related to the review and approval of information technology (IT) policies and procedures remained open.
Supply Chain Risk Management	A prior-year weakness remained open related to the development of a supply chain risk management strategy.
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.

<sup>8</sup> See Appendix C for the status of prior-year recommendations.

<sup>9</sup> See Appendix C for the status of prior-year recommendations.



FY 2024 IG FISMA Metric Domains	Weaknesses Noted
Identity and Access Management	NARA has not effectively transitioned all its information systems (e.g.), major applications and general support systems to use multifactor authentication. In addition, prior year weaknesses related to audit logging, password configuration settings, and account management controls remained open.
Data Protection and Privacy	Prior-year weaknesses remained open related to privacy impact assessments and role-based privacy training.
Information Security Continuous Monitoring (ISCM)	Although NARA has developed, tailored and communicated an ISCM strategy, this strategy is not yet fully integrated with other programs such as supply chain risk management.
Security Training	Prior-year weaknesses remained open related to the completeness of new hire security awareness and privacy training.
Incident Response	NARA has not issued policies and procedures to support event logging (EL) requirements in accordance with OMB M-21-31 <sup>10</sup> requirements and did not reach the EL1, <sup>11</sup> EL2, <sup>12</sup> and EL3 <sup>13</sup> maturity levels by OMB's required due dates.
Contingency Planning	No weaknesses noted.

Source: Sikich's assessment of NARA's information security program controls and practices based on the FY 2024 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** provides agency comments. **Appendix F** provides the report distribution listing.

<sup>10</sup> OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021).

<sup>11</sup> Per OMB M-21-31, EL1 maturity level signifies only logging requirements of highest criticality are met.

<sup>12</sup> Per OMB M-21-31, EL2 maturity level signifies logging requirements of highest and intermediate criticality are met.

<sup>13</sup> Per OMB M-21-31, EL3 maturity level signifies logging requirements at all criticality levels are met.

### III. 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 *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).

#### **Security Function: Identify**

The objective of the Identify function is to develop an organizational understanding of the business context and the resources that support functions that are critical for managing cybersecurity risk to systems, people, assets, data, and capabilities. We determined that the maturity level of NARA's Identify function is Level 1: *Ad Hoc*.

#### ***Metric Domain: Risk Management***

An agency with an effective risk 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 management program.

We determined that the maturity level of NARA's Risk Management domain is Level 2: *Defined*. NARA has not fully implemented components of its agency-wide information security risk management program to meet FISMA requirements. We noted that NARA has three open prior-year recommendations in the Risk Management domain.<sup>14</sup> These weaknesses relate to the review and approval of IT policies, procedures, methodologies, and supplements in accordance with NARA Directive 111, *NARA Directives* and hardware asset inventory management.

The following details the weakness noted in NARA's hardware asset inventory controls.

#### **Hardware Asset Inventory**

NIST standards<sup>15</sup> require NARA to develop and document a comprehensive inventory of information system components that accurately reflects the current information systems, includes all components within the authorization boundary of the system, and is at the level of granularity deemed necessary for tracking and reporting.

We determined that NARA has not consistently used its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the NARA network. Upon examination of NARA's hardware master inventory listing of devices, we noted:

- Seventeen of 3,543 devices in "deployed" status had an incorrect status. Those 17 devices should have been in "move" status rather than "deployed." We determined that these devices had not yet been assigned to an individual and were in storage awaiting future deployment.

---

<sup>14</sup> See Appendix C for additional information regarding these prior-year recommendations.

<sup>15</sup> NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020), security control Configuration Management (CM)-8, Information System Component Inventory.

- One hundred eighty-six of 3,543 devices in “deployed” status, did not have serial numbers noted in the master inventory list. Serial numbers were subsequently identified by management and added into the master inventory listing. We were informed that this data had not been migrated over from the legacy configuration management database hardware asset tracking system.
- Two of 3,543 devices in “deployed” status, did not have user names associated with the equipment. This information was subsequently added to the inventory listing once management was informed.

NARA management indicated that when the previous asset manager was overseeing NARA's IT Support Services contract, their approach involved incorrectly marking any items removed from the central inventory for deployment as “deployed.” This practice was incorrect and went unnoticed. An item should only be marked as “deployed” once it has been issued to the end user. Upon discovery, NARA engaged with a vendor to correct the entries, changing the status from “deployed” to “move.” In addition, inadequate controls over the migration of data from NARA's legacy system which tracked hardware inventory, resulted in incomplete data.

Not following standard data elements required by NARA for asset inventory content, increases the risk that assets may not be adequately tracked and reported, and potentially not adequately secured and protected. In addition, inaccurately tracking hardware assets, increases the risk of misappropriation of assets.

***Recommendations:***

We recommend that the NARA Chief Information Officer (CIO) take the following actions to address prior unimplemented recommendations related to the weaknesses noted for the Risk Management domain.<sup>16</sup>

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. (Recommendation 1, FY 2023 FISMA Audit, Report No. 24-AUD-01)
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. (Recommendation 6, FY 2022 FISMA Audit, Report No. 22-AUD-09)
3. Ensure IT policies, procedures, methodologies, and supplements are reviewed and approved in accordance with NARA Directive 111. (Recommendation 11, FY 2022 FISMA Audit, Report No. 22-AUD-09)

---

<sup>16</sup> The recommendations included are the open prior recommendations which have missed their targeted completion dates related to the Risk Management domain. See Appendix C for status of prior recommendations.

***Metric Domain: Supply Chain Risk Management***

An agency with an effective SCRM program (1) ensures that external providers' products, system components, systems, and services are consistent with the agency's cybersecurity and SCRM requirements, and (2) reports qualitative and quantitative performance measures on the effectiveness of its SCRM program.

We determined that the maturity level of NARA's SCRM domain is Level 1: *Ad-Hoc*. We noted that NARA has one open prior-year recommendation from a previous FISMA report related to the development of a comprehensive SCRM strategy and an implementation plan to guide and govern supply chain risks, as further discussed below.<sup>17</sup>

FISMA requires each federal agency to develop, document and implement Agency-wide strategies, policies, procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and SCRM requirements. As noted in the *Federal Acquisition Supply Chain Security Act of 2018*, agencies are required to assess, avoid, mitigate, accept, or transfer supply chain risks. Also, per Public Law 115-390 – the *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the "SECURE Technology Act"* (12/21/2018) the head of each executive agency is responsible for developing an overall supply chain risk management strategy and implementation plan, policies, and procedures to guide and govern supply chain risk management activities.

As initially reported in the FY 2021 FISMA audit,<sup>18</sup> NARA has not developed a comprehensive SCRM strategy. NARA has drafted policies and procedures to ensure products, components and services adhere to its cybersecurity and SCRM requirements. However, the development of an SRCM strategy and implementation plan have not yet been completed. Therefore, NARA is at risk of implementing policies, procedures, and plans which may not be effectively integrated into NARA's eventual SCRM strategy.

***Recommendations:***

We recommend that the NARA CIO take the following actions to address the prior unimplemented recommendation related to the weaknesses noted for the SCRM domain.<sup>19</sup>

4. Develop and communicate an organization wide Supply Chain Risk Management strategy and implementation plan to guide and govern supply chain risks. (Recommendation 14, FY 2021 FISMA Audit, Report No. 22-AUD-04)

---

<sup>17</sup> See Appendix C for additional information regarding this prior-year recommendation.

<sup>18</sup> Recommendation 14, *National Archives and Records Administration's Fiscal Year 2021 Federal Information Security Modernization Act of 2014 Audit*. (OIG Report No. 22-AUD-04, December 22, 2021).

<sup>19</sup> The recommendation included is the open prior recommendation which has missed its targeted completion date and does include all open recommendations related to the Supply Chain Risk Management domain. See Appendix C for status of prior recommendations.

**Security Function: Protect**

The objective of the Protect function is to develop and implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event. We determined that the maturity level of NARA's Protect function is Level 2: *Defined*.

***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; consistently implements its configuration management policies, procedures, plans, and strategy at all levels of the organization; 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 seven open prior-year recommendations in the Configuration Management domain<sup>20</sup> that relate to improving its vulnerability management program and establishing configuration baseline deviations.

Our independent vulnerability assessment and penetration test during the FY 2024 FISMA audit identified similar issues to open prior-year recommendations related to NARA's vulnerability management program including vulnerabilities related to patch management, configuration management, and unsupported software.

**Vulnerability Management Program**

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (December 10, 2020), security control System and Information Integrity (SI)-2, Flaw Remediation, states that organizations are to install security-relevant software and firmware updates within an organization-defined time period of the release of the updates. Security control Risk Assessment (RA)-5, Risk Assessment, Vulnerability Monitoring and Scanning, states that the organization remediates legitimate vulnerabilities within an organization-defined response time in accordance with an organizational assessment of risk.

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 allow unauthorized access into mission critical systems and data. Many of these vulnerabilities are publicly known and have existed prior to 2023. Furthermore, we identified several instances of unpatched vulnerabilities that NARA was required to patch in accordance with the Cybersecurity & Infrastructure Security Agency's (CISA)<sup>21</sup> Known Exploitable Vulnerability catalog.<sup>22</sup>

---

<sup>20</sup> See Appendix C for additional information regarding these prior-year recommendations.

<sup>21</sup> CISA, a component of DHS, is responsible for cybersecurity and infrastructure protection for all levels of government.

<sup>22</sup> 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 <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> for more details.

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's corrective actions had not been completed.

In addition, during the penetration test, we identified weaknesses related to weak and reused passwords as well as accounts with excessive administrative privileges. We were able to use the password weaknesses to obtain unauthorized access to the accounts with administrator access. We were then able to use the compromised accounts to create a new domain administrator account.

NARA is not reviewing service account passwords to determine if each service account used a unique password. Furthermore, NARA is not reviewing domain user accounts to determine if weak passwords were being used.

The configuration weaknesses increase the risk of an attacker exploiting known vulnerabilities and unauthorized users gaining access to sensitive information. In addition, missing patches and unsupported software increase the risk of weaknesses being exploited and potential 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 his or her actions. If several accounts use the same weak password, a malicious actor can leverage those accounts to further obfuscate their activities.

### ***Recommendations:***

We recommend that the NARA CIO take the following actions, which include the prior unimplemented recommendations related to the weaknesses noted for the Configuration Management domain.<sup>23</sup>

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. (New 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, that the passwords are not found on the list of commonly used, expected, or compromised passwords. (New Recommendation)

---

<sup>23</sup> The recommendation included is the open prior recommendation which has missed its targeted completion date and does include all open recommendations related to the Configuration Management domain. See Appendix C for status of prior recommendations.



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.  
(Recommendation 17, FY 2021 FISMA Audit, Report No. 22-AUD-04)

### ***Metric Domain: Identity and Access Management***

An agency with an effective identity and access management program ensures that all privileged and non-privileged users use strong authentication for accessing organizational systems; employs automated mechanisms to support the management of privileged accounts; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its identity, credential, and access management program.

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 11 open prior-year recommendations in this area.<sup>24</sup> These recommendations relate to audit logging, password configuration settings, shared/group account management, and Identity, Credential, and Access Management (ICAM) strategy. In addition, NARA needs to continue the implementation of multifactor authentication across the agency, as noted below.

#### **User Authentication**

OMB M-19-17<sup>25</sup> states Agencies shall require Personal Identity Verification (PIV) credentials (where applicable in accordance with Office of Personnel Management requirements) as the primary means of identification and authentication to federal information systems, federally controlled facilities, and secured areas by federal employees and contractors.

In addition, NARA's Information Services communicated a requirement for all users (effective April 24, 2023) to use their PIV and accompanying Personal Identification Number for remote access to NARA's network and NARA IT applications. However, the use of PIV or other form of multifactor authentication is not currently mandatory or required for all privileged users, servers and applications, through NARA's Privileged Access Management authentication project and other efforts. In addition, NARA still has ongoing efforts to consolidate physical access control systems and to require PIV or proximity card access for all NARA facilities.

Weaknesses related to authentication mechanisms make it difficult for NARA to ensure that it has adequately secured and protected its information systems and places the systems and the agency at risk for compromise. Specifically, the lack of mandatory multifactor authentication use means information systems are more susceptible to attacks on user accounts.

#### ***Recommendations:***

We recommend that the NARA CIO take the following actions to address prior unimplemented recommendations related to the weaknesses noted for the Identity and Access Management domain.<sup>26</sup>

---

<sup>24</sup> See Appendix C for additional information regarding these prior-year recommendations.

<sup>25</sup> OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential and Access Management* (May 21, 2019).

<sup>26</sup> The recommendations included are the open prior recommendations which have missed their targeted completion date and do not include all open recommendations related to the Identity and Access Management domain. See Appendix C for status of prior recommendations.



8. Implement the following corrective actions:
  - Complete efforts to implement the Security Information and Event Management (SIEM) product.<sup>27</sup>
  - 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. (Recommendation 16, FY 2022 FISMA Audit, Report No.22-AUD-09)
9. Ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy. (Recommendation 17, FY 2022 FISMA Audit, Report No. 22-AUD-09)
10. Ensure audit logging is enabled for each major information system. (Recommendation 19, FY 2022 FISMA Audit, Report No.22-AUD-09)
11. Ensure periodic reviews of generated audit logs are performed for each major information system. (Recommendation 20, FY 2022 FISMA Audit, Report No. 22-AUD-09)
12. Ensure password configuration settings for all major information systems are in accordance with *NARA IT Security Requirements*. (Recommendation 21, FY 2022 FISMA Audit, Report No. 22-AUD-09)
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. (Recommendation 22, FY 2022 FISMA Audit, Report No. 22-AUD-09)
14. Ensure a process is developed, documented, and implemented to change passwords whenever users within shared/group accounts change. (Recommendation 23, FY 2022 FISMA Audit, Report No. 22-AUD-09)
15. Ensure a comprehensive ICAM policy or strategy, which includes the establishment of related Standard Operating Procedures (SOPs), identification of stakeholders, communicating relevant goals, task assignments and measure and reporting progress is developed and implemented. (Recommendation 28, FY 2021 FISMA Audit, Report No. 22-AUD-04)

### ***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 capacities; and reports on qualitative and quantitative data protection and privacy performance measures.

---

<sup>27</sup> SIEM technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting). [Definition of SIEM - IT Glossary | Gartner](#)

We determined that the maturity level of NARA's Data Protection and Privacy domain is Level 2: *Defined*. NARA has defined and communicated policies and procedures related to data encryption, media sanitization and untrusted removable media. However, NARA has three open prior-year recommendations in this area related to completion of privacy impact assessments and ensuring role-based privacy training is completed by all personnel having responsibility for personally identifiable information (PII).<sup>28</sup>

In addition, NARA indicated that an analysis of systems that store sensitive data, implementing encryption of data at rest, and strengthening of its data exfiltration and data loss prevention capabilities are ongoing.

### ***Recommendations:***

No new recommendations are being made for the Data Protection and Privacy domain.<sup>29</sup>

### ***Metric Domain: Security Training***

An agency with an effective security training program identifies and addresses gaps in security knowledge, skills, and abilities; measures the effectiveness of its security awareness and training program; and ensures staff consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.

We determined that the maturity level for NARA's Security Training domain is Level 2: *Defined*. NARA has defined its processes for assessing the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs, and for periodically updating NARA's assessment to account for a changing risk environment. NARA has also implemented policies and procedures that include guidance for role-based training and ensured that role-based specialized training was completed for individuals with significant security responsibilities.

However, as discussed below, we continue to identify weaknesses in the completion of new hire security awareness training related to an open prior-year recommendation in this domain.<sup>30</sup>

### ***New User Security Awareness Training***

Per *NARA Awareness and Training Handbook* (August 15, 2022), all new NARA users must complete an initial security awareness training by reading the IT security threats and the NARA Rules of Behavior (ROB) for access to IT resources within the first 15 days of being issued a network account. The new network accounts are set to automatically expire after 15 days unless the user submits an acknowledgement of reading and understanding the NARA ROB. Once the new NARA personnel, as well as contractors, volunteers, students, and National Archives Foundation and Library support foundation staff submits the acknowledgement, the account is made permanent.

---

<sup>28</sup> See Appendix C for additional information regarding these prior-year recommendations.

<sup>29</sup> No recommendations were noted for the Data Protection and Privacy domain since related open prior-year recommendations had not reached their targeted completion date, and no new recommendations were noted. See Appendix C for status of prior FISMA recommendations.

<sup>30</sup> See Appendix C for additional information regarding these prior-year recommendations

We noted that 2 out of 16 new hires sampled did not complete their new hire security awareness and privacy training or acknowledge their ROB. The users still had active NARA network accounts, despite NARA requirements to automatically expire their accounts after 15 days unless the user submits an acknowledgement of the ROB.

NARA's Learning Management System (LMS) does not provide new hire initial security awareness training briefing, or track completion of it. The initial awareness training briefing is completely separate from LMS. As a result, Information Services indicated that they were working with Human Capital to automate this initial training through a Google form that will provide enhanced workflow processes and tracking of training completion, with additional notices to new users and their supervisors that inform and remind them to complete the training. In addition, NARA is working to ensure that its processes for new user account administration are in alignment with tracking the completion of the initial security awareness training.

Without ensuring new information system users complete security awareness training and acknowledge the ROB prior to gaining systems access, there is an increased risk that system users will not understand their responsibilities when accessing NARA's information systems and managing NARA data. Requiring the completion of the ROB ensures that users read, understand, and agree to follow the rules and limitations related to the systems that they are authorized to access.

### **Recommendations:**

No new recommendations are being made for the Security Training domain.<sup>31</sup>

### **Security Function: Detect**

The objective of the Detect function is to implement continuous monitoring of control activities to discover and identify cybersecurity events in a timely manner. Cybersecurity events<sup>32</sup> include anomalies and changes in the organization's IT environment that may impact organizational operations, including mission, capabilities, or reputation. 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 ISCM program maintains ongoing authorizations of information systems; integrates metrics on the effectiveness of its ISCM program in delivering persistent situational awareness across the organization; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies, procedures, plans, and strategies.

We determined that the maturity level for NARA's ISCM 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 to perform ongoing information security assessments in granting system authorizations, including developing security plans and

---

<sup>31</sup> No recommendations were noted for the Security Training domain since the related open prior-year recommendation had not reached its targeted completion date, and no new recommendations were noted. See Appendix C for status of prior FISMA recommendations.

<sup>32</sup> According to NIST, a cybersecurity event is a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). See [https://csrc.nist.gov/glossary/term/cybersecurity\\_event](https://csrc.nist.gov/glossary/term/cybersecurity_event)

monitoring system security controls. However, although NARA has developed, tailored and communicated an ISCM strategy, this strategy is not yet fully integrated with other programs such as SCRM, as that strategy is still under development. Refer to the SCRM domain section of this report for details related to this finding.

**Recommendations:**

No recommendations are being made for the ISCM domain.

**Security Function: Respond**

The objective of the Respond function is to implement processes to contain the impact of detected cybersecurity events. Such processes include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities. 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.

We determined that the maturity level of NARA's Incident Response domain is Level 3: *Consistently Implemented*. NARA has defined and communicated incident response plans and procedures and consistently implements its processes for incident handling. In addition, NARA has no open prior-year recommendations in this domain. However, NARA has not met EL maturity level requirements, as noted below.

**Event Logging**

OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021),<sup>33</sup> requires federal agencies to improve their investigative and remediation capabilities to ensure that enterprise security operations centers have centralized access to—and visibility into—system logs.

---

<sup>33</sup> See OMB M-21-31 online at <https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf>.

While NARA is developing a plan to assist with reaching compliance with OMB M-21-31 requirements, NARA did not reach the EL1,<sup>34</sup> EL2,<sup>35</sup> and EL3<sup>36</sup> maturity levels by OMB's deadlines as follows:

- Within one year of the date of OMB M-21-31, or by August 27, 2022, achieve the EL1 maturity level.
- Within 18 months of the date of OMB M-21-31, or by February 27, 2023, achieve the EL2 maturity level.
- Within two years of the date of OMB M-21-31, or by August 27, 2023, achieve the EL3 maturity level.

In addition, NARA did not document any risk-based decisions, including compensating controls for not meeting the requirements of OMB M-21-31. NARA management indicated that they are making progress to leverage service offerings from the Department of Justice for a SIEM logging solution to capture security related log events to move NARA towards meeting EL1 maturity level. Therefore, NARA indicated it is in the process of trying to acquire funding to continue this service and expand its SIEM solution to consume more logs going forward.

Cyberattacks underscore the importance of increased government visibility before, during, and after a cybersecurity incident. Information from logs on Federal information systems (for both on-premises systems and connections hosted by third parties, such as cloud service providers) is invaluable in detecting, investigating, and remediating cyber threats. By not achieving the EL maturity levels, NARA is not meeting logging requirements of the highest criticality. NARA is currently at the EL0 maturity level; as such, its EL capabilities are not effective based on OMB M-21-31. Further, NARA may not correlate audit log records across different repositories in a complete or risk-based manner, as defined by OMB M-21-31, which may increase the risk that NARA may not collect all meaningful and relevant data on suspicious events. This may, in turn, increase the risk that NARA may inadvertently miss the potential scope or veracity of suspicious events or attacks.

### ***Recommendations:***

We recommend that the NARA CIO take the following action:

16. Implement requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31. (New Recommendation)

### **Security Function: Recover**

The objective of the Recover function is to develop and implement activities to maintain plans for resilience and to restore capabilities or services that have been impaired due to a cybersecurity incident. The Recover function supports the timely recovery of normal operations to reduce the impact of a cybersecurity incident, including recovery planning, improvements, and communications.

We determined that the maturity level of NARA's Recover function is Level 3: *Consistently Implemented*.

---

<sup>34</sup> Per OMB M-21-31, EL1 maturity level signifies only the logging requirements of highest criticality are met.

<sup>35</sup> Per OMB M-21-31, EL2 maturity level signifies logging requirements of highest and intermediate criticality are met.

<sup>36</sup> Per OMB M-21-31, EL3 maturity level signifies logging requirements at all criticality levels are met.

***Metric Domain: Contingency Planning***

An agency with an effective contingency planning program establishes contingency plans; employs automated mechanisms to thoroughly and effectively test system contingency plans; communicates metrics on the effectiveness of recovery activities to relevant stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures regarding the effectiveness of information system contingency planning program activities.

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 communicated roles and responsibilities related to contingency planning and has consistently implemented those roles and responsibilities across the agency. In addition, we noted that business impact analysis and contingency plans were documented for all sampled systems. Although NARA has consistently implemented contingency planning processes, NARA did not demonstrate how the effectiveness of contingency plans delivers persistent situational awareness across the agency and has not employed automated mechanisms to test system contingency plans more thoroughly and effectively to achieve a higher maturity level.

***Recommendations:***

No recommendations are being made 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 the 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 FIPS 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 December 4, 2023, OMB issued Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the methodology for conducting FISMA evaluations and the processes for federal agencies to report to OMB and, where applicable, DHS. The methodology includes the following:

- OMB selected 17 supplemental IG FISMA Reporting Metrics that IGs must evaluate during FY 2024, in addition to the 20 core IG FISMA Reporting Metrics that IGs must evaluate annually. The remainder of the standards and controls will be evaluated on a 2-year cycle.
- In previous years, IGs have been directed to utilize a mode-based scoring approach to assess maturity levels. Beginning in FY 2023, ratings were focused on calculated average scores, wherein IGs would use the average of the metrics in a particular domain to determine the effectiveness of the individual function areas (i.e., Identify, Protect, Detect, Respond, and Recover). OMB encouraged IGs to focus on the calculated average scores of the 20 core IG FISMA Reporting Metrics, as these tie directly to the administration's priorities and other high-risk areas. In addition, the FY 2024 IG FISMA Reporting Metrics indicated that IGs should use the calculated average scores of the supplemental IG FISMA Reporting Metrics and the agency's progress in addressing outstanding prior-year recommendations as data points to support their risk-based determination of the overall effectiveness of the program and function level.

As highlighted in **Table 3**, the IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and align with the five functional areas in the NIST Cybersecurity Framework, version 1.1: Identify, Protect, Detect, Respond, and Recover.



**Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2024 IG FISMA Reporting Metrics**

Cybersecurity Framework Function Area	Function Area Objective	Domain(s)
<b>Identify</b>	Develop an organizational understanding of the business context and the resources that support critical functions to manage cybersecurity risk to systems, people, assets, data, and capabilities.	<b>Risk Management and SCRM</b>
<b>Protect</b>	Implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event.	<b>Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training</b>
<b>Detect</b>	Implement activities to identify the occurrence of cybersecurity events.	<b>ISCM</b>
<b>Respond</b>	Implement processes to take action regarding a detected cybersecurity event.	<b>Incident Response</b>
<b>Recover</b>	Implement plans for resilience to restore capabilities or services impaired by a cybersecurity event.	<b>Contingency Planning</b>

Source: Sikich's analysis of the NIST Cybersecurity Framework and 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*.

**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 2024 IG FISMA Reporting Metrics

## APPENDIX B: OBJECTIVE, SCOPE, AND METHODOLOGY

### **Objective**

The objective of this performance audit was to assess the effectiveness of NARA's information security program and practices in accordance with FISMA and applicable instructions from OMB and DHS IG FISMA Reporting Metrics.

### **Scope**

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). These 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.

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 2024. The scope also included assessing selected controls from NIST SP 800-53, Revision 5, to support the FY 2024 IG FISMA Reporting Metrics for a sample of 10 systems from a population of 42 systems in NARA's FISMA inventory of information systems as of May 23, 2023.<sup>37</sup>

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 these vulnerability assessment and penetration tests into our FISMA audit results.

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.

The audit covered the period October 1, 2023, through July 30, 2024. We performed audit fieldwork from November 2023 to July 2024.

### **Methodology**

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 2024.
- Focused our testing activities on assessing the maturity of the 20 core and 17 supplemental IG FISMA Reporting Metrics.
- Inspected security policies, procedures, and documentation.

---

<sup>37</sup> NARA's population of FISMA reportable systems included 48 systems as of May 23, 2023, which were identified as a "Major Application" or "General Support System." We further refined this population to exclude OIG and Title 13 systems, resulting in a population of 42 systems for our sample selection.

- Inquired of NARA management and staff.
- Considered guidance contained in OMB's M-24-04, *Fiscal Year 2024 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 10 NARA information systems from the 42 systems in NARA's system inventory. NARA's population of FISMA reportable systems included 48 systems as of May 23, 2023, which were identified as a "Major Application" or "General Support System." We further refined this population to exclude OIG and Title 13 systems, resulting in a population of 42 systems for our sample selection. The ten systems were selected in coordination with the OIG.
- Analyzed the sample of systems selected for testing, including reviewing selected system documentation and other relevant information, as well as evaluated 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 IG FISMA Reporting Metrics introduced a calculated average scoring model that continued for the FY 2024 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, 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 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 2024 IG FISMA Reporting Metrics guidance<sup>38</sup> to form our conclusions for each Cybersecurity Framework 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.

We evaluated the effectiveness of NARA's information security program and practices, with regard to FISMA and related information security policies, procedures, standards, and guidelines, and responded to the FY 2024 IG FISMA Reporting Metrics. 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.

---

<sup>38</sup> The FY 2024 IG FISMA Reporting Metrics provided the agency IG with the discretion to determine the rating for each of the Cybersecurity Framework 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 FISMA REPORT RECOMMENDATIONS

The following is the status of open recommendations from prior FISMA reports. We determined the current status of prior-year FISMA open recommendations by reviewing NARA's overall status for prior-year recommendations and testing the effectiveness of NARA's information security program and practices covering FY 2024.

In addition, NARA closed 5 prior-year recommendations during the audit period. Thus, of 31 open recommendations from prior FISMA reports, 26 recommendations remain open as of July 2024.

### Prior-Year FISMA Recommendations That Were Closed

#### ***NARA'S FISCAL YEAR 2023 FISMA AUDIT OIG REPORT NO. 24-AUD-01***

Number	Recommendation
2	Ensure complete security authorization packages for each major application and general support system is completed prior to deployment into production.
4	Document Information Services review of Cross-site Request Forgery tokens for external web applications and if an issue is identified, document the remediation efforts or other existing mitigations in place to protect against cross site forgery requests.
10	Document, communicate and implement NARA's configuration management processes applicable to all NARA systems, not just those under Enterprise Change Advisory Board control, within NARA's Configuration Management program management plan or other NARA methodology.

#### ***NARA'S FISCAL YEAR 2022 FISMA AUDIT OIG REPORT NO. 22-AUD-09***

Number	Recommendation
14	We recommend the CIO ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported. (This recommendation was subsumed into report No. 24-AUD-01, recommendation 8) <sup>39</sup>
18	Ensure upon termination of employment, all system access is disabled in accordance with the applicable system security plan defined period, as described under control PS-4 "Personnel Termination."

<sup>39</sup> Recommendation 14 from Audit Report No. 22-AUD-09 was closed and subsumed into recommendation 8 from Audit Report No. 24-AUD-01, as both recommend the migration of information systems away from unsupported operating systems to operating systems that are vendor-supported.

## Prior-Year FISMA Recommendations That Remain Open

**NOTE:** These remaining open recommendations do not represent—and are not intended to represent—all recommendations within the respective years or reports identified.

### ***NARA'S FISCAL YEAR 2023 FISMA AUDIT OIG REPORT NO. 24-AUD-01***

Number	Recommendation	Metric Domain Impacted
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.	Risk Management
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.	Configuration Management
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.	Configuration Management
6	Implement remediation efforts to address security deficiencies on affected systems identified, to include enhancing its patch and vulnerability management program as appropriate, or document acceptance of the associated risks.	Configuration Management
7	Document and implement a process to track and remediate persistent configuration vulnerabilities or document acceptance of the associated risks.	Configuration Management
8	Ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported.	Configuration Management
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.	Configuration Management
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.	Security Training
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.	Identity and Access Management
13	Enforce mandatory PIV card authentication for all NARANet users, in accordance with OMB requirements.	Identity and Access Management

Number	Recommendation	Metric Domain Impacted
14	Ensure NARANet user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements.	Identity and Access Management
15	Ensure that the Senior Agency Official for Privacy (SAOP) complete Privacy Impact Assessments for all systems which contain PII.	Data Protection and Privacy
16	The SAOP review and update NARA's 1609 Initial Privacy Reviews and Privacy Impact Assessments privacy policies and procedures to reflect NARA's current processes and controls.	Data Protection and Privacy
17	The CIO and SAOP 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.	Data Protection and Privacy

**NARA'S FISCAL YEAR 2022 FISMA AUDIT  
OIG REPORT NO. 22-AUD-09**

Number	Recommendation	Metric Domain Impacted
6	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. (Prior audit Report No. 22-AUD-04, recommendation 6)	Risk Management
11	Ensure IT policies, procedures, methodologies, and supplements are reviewed and approved in accordance with NARA Directive 111. (Prior audit Report No. 22-AUD-04, recommendation 11)	Risk Management
16	Implement the following corrective actions: <ul style="list-style-type: none"> <li>Complete efforts to implement the SIEM product.</li> <li>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.</li> <li>Ensure the procurement of new IT system hardware and software, which provides user authentication, includes a minimum set of audit logging. (Prior audit Report No. 22-AUD-04, recommendation 16)</li> </ul>	Identity and Access Management
17	Ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy. (Prior audit Report No. 22-AUD-04, recommendation 17)	Identity and Access Management



Number	Recommendation	Metric Domain Impacted
19	Ensure audit logging is enabled for each major information system. (Prior audit Report No. 22-AUD-04, recommendation 19)	Identity and Access Management
20	Ensure periodic reviews of generated audit logs are performed for each major information system.	Identity and Access Management
21	Ensure password configuration settings for all major information systems are in accordance with NARA IT Security Requirements.	Identity and Access Management
22	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.	Identity and Access Management
23	Ensure a process is developed, documented, and implemented to change passwords whenever users within shared/group accounts change.	Identity and Access Management

**NARA'S FISCAL YEAR 2021 FISMA AUDIT  
OIG REPORT No. 22-AUD-04**

Number	Recommendation	Metric Domain Impacted
14	Develop and communicate an organization wide Supply Chain Risk Management strategy and implementation plan to guide and govern supply chain risks.	Supply Chain Risk Management
17	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.	Configuration Management
28	Ensure a comprehensive 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.	Identity and Access Management



**APPENDIX D: ACRONYMS**

Acronym	Definition
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
DHS	Department of Homeland Security
EL	Event Logging
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ICAM	Identity Credential and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
LMS	Learning Management System
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
ROB	Rules of Behavior
SAOP	Senior Agency Official for Privacy
SCRM	Supply Chain Risk Management
SIEM	Security Information and Event Management
SOP	Standard Operating Procedure
SP	Special Publications

**APPENDIX E: AGENCY COMMENTS**

Agency management reviewed the draft audit report and provided no comments to this report. Agency management stated their general agreement with the findings and recommendations and opted not to provide formal comments for inclusion in this report.

**APPENDIX F: REPORT DISTRIBUTION LIST**

Archivist of the United States

Deputy Archivist of the United States

Executive Secretariat

Acting Chief Operating Officer

Acting Chief of Management and Administration

Deputy Chief Operating Officer

Chief Financial Officer

Chief Information Officer

Deputy Chief Information Officer

Accountability

United States Senate Homeland Security and Governmental Affairs Committee

United States House of Representatives Committee on Oversight and Reform

## OIG HOTLINE 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. Walk-ins are always welcome. Visit [www.archives.gov/oig/](http://www.archives.gov/oig/) or <https://naraoig.oversight.gov/> for more information, or contact us:

**By telephone**

Washington, DC, Metro area: 301-837-3000

Toll-free: 800-786-2551

**By facsimile**

301-837-3197

**By online referral form**

<https://naraoig.oversight.gov/online-complaint-form>

**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 <https://naraoig.oversight.gov/online-complaint-form>.