NATIONAL ARCHIVES | Inspector General

October 24, 2023

TO: Dr. Colleen Shogan
Archivist of the United States

FROM: Dr. Brett M. Baker Brett M Baker
Inspector General

SUBJECT: *National Archives and Records Administration's Fiscal Year 2023 Federal Information Security Modernization Act of 2014 Audit*
OIG Report No. 24-AUD-01

The Office of Inspector General (OIG) contracted with CliftonLarsonAllen, LLP (CLA) 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 2023. Based upon the audit of NARA's information security program, including its compliance with FISMA and OMB/DHS requirements in the function areas, CLA concluded that NARA's information security program was "Not Effective." In addition, NARA's overall maturity level improved to a level of "Consistently Implemented." The report contains three new recommendations and 14 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.

CLA is responsible for the attached auditor's report dated October 23, 2023 and the conclusions expressed in the report. The findings and conclusions presented in the report are the responsibility of CLA. 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 amend*ed, we will provide copies of our report to congressional committees with oversight responsibility over NARA.

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

Attachment

cc: Debra Steidel Wall, Deputy Archivist of the United States
Tasha Ford, Executive Secretariat
Gary M. Stern, General Counsel
Micah Cheatham, Chief of Management and Administration
William Bosanko, Chief Operating Officer
Meghan Guthorn, Deputy Chief Operating 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

National Archives and Records Administration's
Fiscal Year 2023
Federal Information Security Modernization Act of 2014 Audit

Final Report

October 23, 2023

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
National Archives and Records Administration

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the National Archives and Records Administration's (NARA's) information security management program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA or Act) for fiscal year (FY) 2023. FISMA requires agencies to develop, implement, and document an Agency-wide information security program and practices. The Act also requires Inspectors General (IGs) to conduct an annual review of their agencies' information security programs and practices and report the results to the Office of Management and Budget (OMB).

The objective of this 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.

For FY 2023, OMB required IGs to assess 20 Core and 20 Supplemental IG FISMA Reporting Metrics in five security function areas – Identify, Protect, Detect, Respond, and Recover – to determine the effectiveness of their agencies' information security programs and practices 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 and practices must be rated Level 4 – *Managed and Measurable*.

Our audit was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To address the FY 2023 IG FISMA Reporting Metrics, we reviewed select controls for a sample of 10 NARA FISMA reportable systems, performed an internal and external vulnerability assessment and penetration test, interviewed agency officials, and reviewed data including system security and privacy documentation. We also reviewed the status of the 47 open FISMA prior-year recommendations related to NARA's information security program and practices. We performed audit fieldwork which covered NARA's headquarters located in College Park, MD, from January 2023 to August 2023. The audit covered the period from October 2022 through August 2023.

Based upon 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, one functional area (Identify) achieved a maturity level of "Ad Hoc," one functional area (Protect) achieved a maturity level of "Defined," and three functional areas (Detect, Respond and Recover) achieved a maturity level of "Consistently Implemented" for an overall maturity level of "Consistently Implemented" for the security program. Thus, NARA's overall maturity level has changed from last year, with three of nine domains remaining at the same maturity level as last year (Risk Management, Supply Chain Risk Management, and Security Training). However, NARA has improved maturity levels for six of nine domains (Configuration Management, Identity and Access Management, Data Protection, and Privacy Information Security Continuous Monitoring, Incident Response and Contingency Planning). NARA continues to stress its commitment to improving information security throughout the agency and is making steady progress to that end in the areas of security assessment and authorization documentation controls, and contingency plan documentation and testing.

We made three new recommendations and included within the body of the report 14 repeat recommendations from prior year FISMA audits (which had missed their targeted completion dates) to help NARA address challenges in its development of a mature and effective information security program and practices. In addition, we noted another 14 recommendations related to prior FISMA audits are still open which have not missed their target completion date, and 19 recommendations were closed.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. The information in this report was obtained from NARA on or before October 23, 2023. We have no obligation to update our report or to revise the information contained herein to reflect events occurring after October 23, 2023.

The purpose of this audit report is to report on our assessment of NARA's compliance with FISMA and is not suitable for any other purpose.

Additional information on our findings and recommendations is included in the accompanying report.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
October 23, 2023

Table of Contents

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
2023 FISMA AUDIT

Executive Summary

The Federal Information Security Modernization Act of 2014[1] (FISMA or Act) requires federal agencies to develop, document, and implement an agency-wide information security program and practices 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) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct a performance audit in support of the FISMA requirement for an annual independent evaluation of NARA's information security program and practices for fiscal year (FY) 2023. The objective of this performance audit was to determine 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.[2]

The FY 2023 IG FISMA Reporting Metrics requires us to assess the maturity of five functional areas in the Agency's information security programs and practices. For this year's review, IGs were required to assess 20 Core[3] IG FISMA Reporting Metrics and 20 Supplemental[4] IG FISMA Reporting Metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover – to determine the effectiveness of their agencies' information security program and practices and the maturity level of each function area.[5] 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 and practices must be rated Level 4 – *Managed and Measurable*.

To address the FY 2023 IG FISMA Reporting Metrics, we reviewed select controls for a sample of 10 NARA FISMA reportable systems, interviewed agency officials, and reviewed information, including system security documentation. Refer to Appendix A for background on the FISMA legislation and Appendix B for details on our audit objective, scope, and methodology. We also reviewed the status of the 47 open FISMA prior-year recommendations related to NARA's security program and practices. Appendix C contains the current-year status of prior FISMA recommendations. Appendix D provides a listing of acronyms used throughout this report. Appendix E provides agency comments.

The audit was performed in accordance with generally accepted government auditing standards. Those standards require that the auditor plan and perform the audit to obtain sufficient,

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] We submitted our responses to the FY 2023 IG FISMA Reporting Metrics to NARA OIG as a separate deliverable under the contract for this performance audit.

[3] 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.

[4] Supplemental Metrics are assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

[5] The function areas are further broken down into nine domains.

appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Audit Results

Based upon 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." The following five domains were assessed at the "Defined" level (Risk Management, Security Training, Information Security Continuous Monitoring, Incident response, and Contingency Planning). In addition, the following four domains were assessed at the "Ad Hoc" level (Supply Chain Risk Management, Configuration Management, Identity and Access Management, and Data Protection and Privacy) as noted in **Table 1** below.

Table 1: FY 2023 IG Cybersecurity Framework Function and Domain Ratings

Cybersecurity Framework Security Functions[6]	FY 2023 Maturity Level by Function	Metric Domains	Domain Maturity Level	Change from FY 2022
Identify	Ad Hoc (Level 1)	**Risk Management**	Defined (Level 2)	No Change
		Supply Chain Risk Management	Ad Hoc (Level 1)	No Change
Protect	Defined (Level 2)	**Configuration Management**	Defined (Level 2)	Upgraded from Ad Hoc (Level 1)
		Identity and Access Management	Defined (Level 2)	Upgraded from Ad Hoc (Level 1)
		Data Protection and Privacy	Defined (Level 2)	Upgraded from Ad Hoc (Level 1)
		Security Training	Defined (Level 2)	No Change
Detect	Consistently Implemented (Level 3)	**Information Security Continuous Monitoring**	Consistently Implemented (Level 3)	Upgraded from Defined (Level 2)
Respond	Consistently Implemented (Level 3)	**Incident Response**	Consistently Implemented (Level 3)	Upgraded from Defined (Level 2)
Recover	Consistently Implemented (Level 3)	**Contingency Planning**	Consistently Implemented (Level 3)	Upgraded from Defined (Level 2)
Overall	**Level 3: Consistently Implemented - Not Effective**			

[6] 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.

While NARA's security program did not reach an effective level, NARA continues to stress its commitment to improving information security throughout the agency and is making steady progress to that end in the areas of security assessment and authorization documentation controls, and contingency plan documentation and testing. Specifically, NARA continued its progress toward a more mature information security program and practices, including the following:

- Information Services has updated their security methodologies and IT security handbooks to address inconsistencies.
- Improvements were made in the process of documenting digital identity risk assessments.
- Improvements were made with documentation of system controls within information system security plans.
- Improvements were made in updating policies and procedures and related management and documentation of plans of actions and milestones.

However, to fully progress towards "Consistently Implemented," NARA will need to address the weaknesses in its policies and procedures to ensure they are accurate, complete, consistent, and communicated to all information security stakeholders. Consistent implementation of security controls throughout the agency can only be achieved when there are sound and reliable policies and procedures, as the foundational levels of a mature information security program and practices. Additionally, NARA needs to ensure:

- Multi factor authentication is enforced agency wide.
- User account management processes related to documentation, account monitoring, and the separation process are strengthened.
- System patch and configuration vulnerabilities are remediated in a timely manner, and improved processes are developed to address unsupported software.

NARA's information security program and practices has longstanding weaknesses in developing and consistently implementing policies and procedures. These weaknesses are mostly in the areas of configuration management, specifically vulnerability management remediation, account management and authentication such as fully implementing multi-factor authentication and ensuring inactive accounts are disabled timely, and development and implementation of a supply chain risk management strategy.

To demonstrate measurable improvements towards an effective information security program and practices, NARA needs to improve its performance monitoring to ensure controls are operating as intended for all systems. Additionally, NARA needs to communicate security deficiencies to the appropriate personnel, who should take responsibility for developing corrective actions and ensuring those actions are implemented.

At present, the weaknesses that we identified (as summarized in **Table 2** below) leave NARA operations and assets at risk of unauthorized access, misuse, and disruption. Although the majority of these weaknesses were similar to prior year reported weaknesses,[7] with 28 recommendations remaining open, we made three new recommendations to help NARA address challenges in its development of a mature and effective information security program and practices. We included within the body of the report 14 repeat recommendations from prior year FISMA audits (which had missed their targeted completion dates) to help NARA address

[7] *National Archives and Records Administration's Fiscal Year 2022 Federal Information Security Modernization Act of 2014 Audit.* OIG Report Number 22-AUD-09 (9/29/22).

challenges in its development of a mature and effective information security program and practices. In addition, we noted a different 14 recommendations related to prior FISMA audits are still open which have not missed their target completion date, and 19 recommendations were closed.

Table 2: Weaknesses Noted in FY 2023 FISMA Audit Mapped to Domains in the FY 2023 IG FISMA Metrics

FY 2023 IG FISMA Metric Domains	Weaknesses Noted
Risk Management	Security Assessment and Authorization (SA&A) documentation was incomplete.
Supply Chain Risk Management	The prior-year weakness related to there being no supply chain risk management strategy/plan remained open.
Configuration Management	Ineffective patch and vulnerability management process for remediation of vulnerabilities.
	Prior-year weaknesses remained open related to configuration management plans and policies were not consistently maintained.
Identity and Access Management	Incomplete enforcement of two-factor user authentication mechanisms.
	Disabling of inactive user accounts and in a timely manner upon separation of employment.
	Prior-year weaknesses remained open related to the development of a comprehensive Identity, Credentialing and Access Management (ICAM) policy or strategy.
Data Protection and Privacy	Prior-year weaknesses remained open related to the implementation of tools to strengthen data loss protection, privacy policy and procedure updates, and role-based privacy training.
Information Security Continuous Monitoring	SA&A documentation was incomplete.
Security Training	Prior-year weaknesses remained open related to specialized role-based privacy training as noted under the Data Protection and Privacy domain.
Contingency Planning	None

The following section, FISMA Audit Findings, provides a detailed discussion of the audit findings grouped by the Cybersecurity Framework Security Functions. In addition, subsequent appendices provide more details on the FISMA legislation, audit scope and methodology, prior year recommendations, system selections, and acronyms utilized throughout this report.

- FISMA audit findings.
- Appendix A describes background information on the FISMA legislation.
- Appendix B describes the audit objective, scope, and methodology.
- Appendix C contains the current year status of prior FISMA report recommendations.
- Appendix D provides a listing of acronyms utilized throughout this report.
- Appendix E provides agency comments.
- Appendix F provides the report distribution listing.

FISMA Audit Findings

Security Function: Identify

Overview

NARA developed and published various directives, IT security requirements and handbooks to describe its entity-wide information security risk management program and Risk Management Framework (RMF). The RMF addressed both security and privacy controls. NARA's information security risk management process focused on identifying and evaluating the threats to and vulnerabilities of NARA information. The RMF also focused on identifying risk management and mitigation strategies to address these threats and vulnerabilities. However, NARA's risk management process was not fully effective since weaknesses and inconsistent implementation of the policies and procedures continue to exist.

Metric Domain – Risk Management

FISMA requires each federal agency to develop, document, and implement an agency-wide information security and risk management program. Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, agencies should assess the likelihood that an event will occur and the resulting impact. With this information, agencies can determine the acceptable level of risk for delivery of services and can set their risk tolerance.

NARA has not fully implemented components of its Agency-wide information security risk management program to meet FISMA requirements. The policies, procedures, and documentation included in the NARA enterprise risk management program were not consistently implemented or applied across all NARA systems. NARA has defined its processes to perform ongoing information security assessments granting system authorizations, including developing security plans and monitoring system security controls. However, we noted these procedures were not being communicated or consistently performed across NARA, resulting in two of ten sampled systems which did not have a finalized Authorization to Operate (ATO) although a draft ATO was provided, and the authorization was going through stakeholder approvals.

NIST Special Publications (SP) 800-37, Revision 2, *Risk Management Framework to Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* is guidance for applying the RMF controls. The six step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The goal of the RMF is to provide near real-time risk management and ongoing authorization of information systems through robust continuous monitoring processes.

The following details the weaknesses noted in NARA's risk management framework.

<u>Security Assessment and Authorization</u>

NARA policy requires system owners to annually assess security controls for their information systems and operating environments and examine the following security documentation: system security plan, security assessment report, and security assessment plan.

However, we noted that 2 of 10 sampled systems, have been in operation without a complete security authorization package to include an ATO signed by the authorizing official, due to management concerns about the legacy, out of support software used in the technology platforms which these systems reside upon.

Delay in the finalization of the ATO was attributed to concerns about the risk inherent in the technology platform which the affected system resides upon. NARA management indicated that a draft ATO has been developed and is going through stakeholder approvals. Considering authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems, the continued use of systems which have not received an authorization to operate, could present an ongoing risk to NARA and its assets since associated risks were not adequately accepted or mitigated.

Recommendations:

We recommend 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:[8]

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 #13 from FY 2021 FISMA audit, report #22-AUD-04)

2. Ensure complete security authorization packages for each major application and general support system is completed prior to deployment into production. (Recommendation #1 from FY 2022 FISMA audit, report #22-AUD-09)

Metric Domain – Supply Chain Risk Management

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 supply chain risk management 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*" (12/31/18) 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,[9] NARA has not developed a comprehensive Supply Chain Risk Management (SCRM) strategy. NARA has developed policies and procedures related to procurements and contracting to manage supply chain risks and indicated that as part of ongoing updates to their IT security policy documents, NARA is including requirements for the new supply chain security controls. The actual development of an SCRM strategy and implementation plan however has not yet been completed and NARA indicated they are in the early stages of documenting their SCRM strategy.

[8] The recommendations included are the open prior recommendations which have missed their targeted completion dates and do not include all open recommendations related to the Risk Management domain. See Appendix C for status of prior recommendations.

[9] *National Archives and Records Administration's Fiscal Year 2021 Federal Information Security Modernization Act of 2014 Audit*. OIG Report Number 22-AUD-04 (12/22/21), Recommendation #14.

As a result, NARA is at risk of implementing policies, procedures, and plans which may not be effectively integrated into NARA's eventual supply chain risk management strategy.

Recommendations:

No recommendations are being made for the Supply Chain Risk Management domain.[10]

[10] No recommendations were provided for the Supply Chain Risk Management domain since the targeted completion date for its related open prior year recommendation had not yet occurred, and no new recommendations were identified during FY 2023. See Appendix C for status of prior recommendations, organized by fiscal year report.

Security Function: Protect

Overview

NARA's Protect controls which cover configuration management, identity and access management, data protection and privacy, and security training were not effective and not consistently implemented across NARA. In FY 2023, weaknesses in the NARA IT environment continue to contribute to deficiencies in system configuration, data protection and privacy, and access controls.

The following details the weaknesses noted in NARA's configuration management domain.

Metric Domain – Configuration Management

NARA continues to have incomplete and inconsistent documentation of its configuration management policies and procedures. Specifically, configuration and patching weaknesses persist, a comprehensive enterprise-wide configuration management information security policy does not exist, and configuration management plans were not developed for all systems.

Vulnerability Management Program

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, 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 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 and penetration testing assessments of NARA's network and a sample of 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 have existed and been publicly known from 2022 and before.

As a result, NARA's internal vulnerability scan processes were not effective in tracking and remediating configuration vulnerabilities identified in network devices. In addition, management did not ensure devices deployed within NARA's network were hardened to prevent default or weak authentication mechanisms.

Information Services had a patch and vulnerability management program in place; however, it was not effective in tracking and remediating all needed software patches and upgrades in a timely manner. Despite software vendors announcing upcoming end of service dates for their products months and sometimes years in advance, NARA's Information Services efforts were delayed for remediation of unsupported software. Information Services was aware of the unsupported software and an application management group was tracking the unsupported software and remediation efforts. However, based on available resources, system requirements, and related constraints the remediation efforts were delayed.

An attacker may exploit the vulnerabilities identified during the testing to take control over certain systems, cause a denial-of-service attack, or gain unauthorized access to critical files and data.

In addition, the inconsistent application of vendor patches could jeopardize the data integrity and confidentiality of NARA's sensitive information. Without remediating all significant security vulnerabilities, systems could be compromised, resulting in potential harm to data confidentiality, integrity, and availability.

Configuration Compliance Management

NARA's *Configuration Compliance Management Standard Operating Procedure* requires Information System Security Officers (ISSO) to review monthly system configuration compliance scans and to track progress of unapproved deviations in a system plans of action and milestones (POA&M). However, we noted that ISSO's were not reviewing these reports on a monthly basis or creating POA&Ms for the baseline issues as required. The lack of monthly reviews and adding baseline related POA&Ms was due to the documentation of these procedures after the current ISSO contract was procured.

By not accurately monitoring deviations from approved baseline configurations, system baseline configurations could be changed and go unnoticed. This could lead to insecure system configurations and may result in vulnerabilities for NARA systems.

Although a *Configuration Compliance Management Standard Operating Procedure* (SOP) has been developed which includes a configuration management plan template and security baseline/ baseline deviation processes, the configuration management plans for systems were still under development using this template.

Recommendations:

We recommend the NARA CIO take the following actions which include the prior unimplemented[11] recommendations related to the weaknesses noted for the Configuration Management domain:

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. (New Recommendation)

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. (Recommendation #12 from the FY 2022 FISMA audit, report 22-AUD-09)

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. (Recommendation #13 from the FY 2022 FISMA audit, report #22-AUD-09)

6. Implement remediation efforts to address security deficiencies on affected systems identified, to include enhancing its patch and vulnerability management program as

[11] The prior unimplemented recommendations included are the open prior recommendations which have missed their targeted completion dates and do not include all open recommendations related to the Configuration Management domain. See Appendix C for status of prior recommendations.

appropriate, or document acceptance of the associated risks. (Recommendation #16 from the FY 2021 FISMA audit, report #22-AUD-04)

7. Document and implement a process to track and remediate persistent configuration vulnerabilities or document acceptance of the associated risks. (Recommendation #15 from the FY 2021 FISMA audit, report #22-AUD-04)

8. Ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported. (Recommendation #18 from the FY 2021 FISMA audit, report #22-AUD-04)

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. (Recommendation #22 from the FY 2021 FISMA audit, report #22-AUD-04)

10. Document, communicate and implement NARA's configuration management processes applicable to all NARA systems, not just those under Enterprise Change Advisory Board (ECAB) control, within NARA's Configuration Management (CM) program management plan or other NARA methodology. (Recommendation #15 from the FY 2022 FISMA audit, report #22-AUD-09)

Metric Domain – Identity and Access Management

Proper identity and access management ensures users and devices are properly authorized and authenticated to access information and information systems. In addition, policy and procedures must be in place for the creation, provisioning, maintenance, and eventual termination of accounts. Homeland Security Presidential Directive 12 calls for all federal departments and agencies to require personnel to use personal identity verification (PIV) cards as a major component of a secure, government-wide account and identity management system.

User Authentication

OMB M-11-11[12] required agencies to develop and issue an implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems.

In addition, OMB M-19-17[13] states Agencies shall require PIV credentials (where applicable in accordance with OMB requirements) as the primary means of identification and authentication to federal information systems, federally controlled facilities, and secured areas by federal employees and contractors.

Specifically, we noted that on April 24, 2023, NARA required all users to use their PIV and accompanying Personal Identification Number (PIN) for remote access to the NARA network and NARA IT applications. However, the use of PIV or other form of multi factor authentication for local privileged and non-privileged user access to the NARA network, is not currently mandatory or required for all privileged users, servers and applications, through NARA's Privileged Access

[12] OMB Memorandum M-11-11, *Continued Implementation Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractors (February 3, 2011)*.

[13] OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential and Access Management (May 21, 2019)*.

Management authentication project and other efforts. In addition, we noted that only 11 (9%) of 124 users assigned privileged NARA network accounts were configured as PIV required for authentication.

NARA is still completing the migration of an identity security and access management tool to require PIV authentication for all users, servers, and applications.

Unresolved weaknesses in identity and access management, particularly pertaining to authentication mechanisms, make it difficult for NARA to ensure its information systems are adequately secured and protected and place the agency at risk for compromise. Specifically, the missing mandatory PIV/multifactor authentication means information system are more susceptible to attacks on user accounts.

Account Management

NARA policy requires that when a user separates or terminates from NARA, and no longer needs access to NARANet, their account is disabled after 60 days, after 90 days the user is deprovisioned, then if deprovisioned for over 180 days they will be removed from the system.

However, Information Services indicated that there are no automated mechanisms in place to disable inactive privileged NARA network user accounts. Due to an oversight by management, several individuals that separated from NARA employment, or contractors no longer required access, had system accounts not disabled within 90 days as required by NARA policy.

In addition, NARA did not effectively manage new hire training and review user accounts for certain major applications and general support systems in audit scope. Specifically, the following issues were noted:

- 3 of a total of 18 NARA network privileged administrator user accounts that were inactive for more than 90 days, were not disabled in accordance with NARA policies. We confirmed these accounts were subsequently disabled.

- For 2 application users that separated employment from NARA during the audit period; their user accounts were not disabled or deleted. We confirmed those accounts were subsequently deleted after identification.

- 7 out of 10 new hires sampled did not complete their new hire training with associated acknowledgement of Rules of Behavior and did not have their NARA network system access disabled, as a result.

Privileged roles are assigned to individuals that are allowed to perform certain security-relevant functions that ordinary users are not authorized to perform. Therefore, inadequate privileged account management and infrequent review and monitoring increases the risk of a lack of accountability and account misuse to violate NARA’s information systems parameters.

If user accounts are maintained and not timely disabled after an employee’s departure, there is a risk that these accounts could be accessed by unauthorized users. Although a PIV card is required to authenticate users to the network and PIV cards are required to be cancelled upon separation, maintaining remote account access after separation poses the risk that such active accounts may be targeted for exploitation. Unauthorized users could use an account to gain access to NARA’s information systems.

If NARA system users do not receive initial security awareness training and complete the Rules of Behavior, there is an increased risk that those individuals may not take adequate precautions to ensure NARA data and systems are effectively protected from unauthorized access, modification, or deletion.

In addition, a crucial part of an identity and access management program includes the development of an identity, credential, and access management (ICAM) program. Specifically, OMB M-19-17 requires each agency to define and maintain a single comprehensive ICAM policy, process, and technology solution roadmap, consistent with agency authorities and operational mission needs. These items should encompass the agency's entire enterprise; align with the Government-wide federal ICAM Architecture and Continuous Diagnostics Management requirements; incorporate applicable federal policies, standards, playbooks, and guidelines; and include roles and responsibilities for all users.

However, we noted that previously reported weaknesses and recommendations related to an ICAM charter remained open during FY 2023. Although NARA has developed an ICAM Executive Board Charter which was signed by the Archivist, there were still actions to be completed by the targeted September 2023 completion date such as the establishment of an ICAM governance board, development, and implementation of operational SOPs.

Although NARA has defined its process for provisioning, managing, and reviewing privileged accounts, previously reported weaknesses related to the timely removal of system access for separated individuals and inactive user accounts, and documenting audit log reviews were not resolved as planned corrective actions were still ongoing.

Recommendations:

We recommend the NARA CIO take the following actions which include the prior unimplemented[14] recommendations related to the weaknesses noted for the Identity and Access Management domain.

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. (New Recommendation)

12. Continue and complete efforts to require PIV authentication for all privileged users, servers and applications, through NARA's Privileged Access Management authentication project and other efforts. (Recommendation #26 from the FY 2021 FISMA audit, report #22-AUD-04)

13. Enforce mandatory PIV card authentication for all NARANet users, in accordance with OMB requirements. (Recommendation #27 from the FY 2021 FISMA audit, report #22-AUD-04)

[14] The prior unimplemented recommendations included are the open prior recommendations which have missed their targeted completion dates and do not include all open recommendations related to the Identity and Access Management domain. See Appendix C for status of prior recommendations.

14. Ensure NARANet user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements. (Recommendation #29 from the FY 2021 FISMA audit, report #22-AUD-04)

Metric Domain – Data Protection and Privacy

FISMA requires the federal government to establish a privacy program and corresponding policies and procedures for the protection of Personally Identifiable Information (PII) collected, used, maintained, shared, and disposed of by information systems. NARA's 1609 *Initial Privacy Reviews and Privacy Impact Assessments* transmittal memo directive requires a Privacy Impact Assessment (PIA) for all NARA owned IT systems and new electronic information collections. Also, per Executive Order 14028, *Improving the Nations Cybersecurity*, agencies are required to limit the transference of data by removable media.

We noted the following weaknesses related to NARA's data protection and privacy controls:

- For 3 of 10 sampled NARA systems which contain PII, a PIA was not completed.

- The Senior Agency Official for Privacy (SAOP) has not yet reviewed and updated the *NARA 1609 Initial Privacy Reviews and Privacy Impact Assessments* privacy policies and procedures since 2009 to reflect NARA's current processes and controls.

As the security assessment and authorization package developed for two of the systems, was still in progress, this resulted in the delayed finalization and approval of the PIAs. In addition, NARA has indicated that they are still in the process of reviewing and approving NARA's privacy policies.

If a PIA is not completed for a system which handles PII, there is an increased risk that inadequate physical and technical safeguards are in place to protect information from inappropriate disclosure.

Also, the NARA Cybersecurity Handbook does not include sufficient detail on its policies and procedures related to data exfiltration, enhanced network defenses, email authentication processes, and mitigation against Domain Name Service (DNS) infrastructure tampering. In addition, NARA management indicated that plans and efforts to strengthen exfiltration and Data Loss Prevention (DLP) capabilities were still in progress, and not yet funded in FY 2023. If NARA policies and procedures are not updated and implemented, there is an increased risk of data exfiltration of information from systems and the introduction of malicious code.

In addition, previously reported weaknesses and recommendations[15] related to role-based privacy training for all individuals having responsibility for PII remained open during FY 2023.

Recommendations:

We recommend the NARA CIO coordinate with the SAOP to take the following actions which include the prior unimplemented[16] recommendations related to the weaknesses noted for the Data Protection and Privacy domain.

[15] *National Archives and Records Administration's Fiscal Year 2021 Federal Information Security Modernization Act of 2014 Audit.* OIG Report Number 22-AUD-04 (12/22/21), Recommendation #34.

[16] The prior unimplemented recommendations included are the open prior recommendations which have missed their targeted completion dates and do not include all open recommendations related to the Data Protection and Privacy domain. See Appendix C for status of prior recommendations.

15. Ensure that the SAOP complete PIAs for all systems which contain PII. (New Recommendation)

16. The SAOP review and update the *NARA 1609 Initial Privacy Reviews and Privacy Impact Assessments* privacy policies and procedures to reflect NARA's current processes and controls. (Recommendation #33 from the FY 2021 FISMA audit, report #22-AUD-04)

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, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements. (Recommendation #34 from the FY 2021 FISMA audit, report #22-AUD-04)

Metric Domain – Security Training

FISMA requires organizations assess the skills, knowledge, and abilities of their personnel to provide specific awareness and specialized security training to equip personnel to perform their responsibilities and safeguard NARA's assets, IT data, and resources.

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. However, as noted under the Account Management section, training for new hires was not always performed in a timely manner. We noted that although NARA demonstrated security awareness training was completed for all new hires sampled, it was not always completed in a timely manner. In addition, the prior-year audit[17] identified role-based training weaknesses within the data protection and privacy domain section that remain open.

Control weaknesses in the security training domain expose NARA to increased risk of unintentional and insecure user behavior in protecting the technology environment. Thus, NARA may not have reasonable assurance regarding the confidentiality and integrity of information in its systems.

Recommendations:

No recommendations are being made for the Security Training domain.[18]

[17] *National Archives and Records Administration's Fiscal Year 2021 Federal Information Security Modernization Act of 2014 Audit.* OIG Report Number 22-AUD-04 (12/22/21), Recommendation #34.

[18] No recommendations were noted for the Security Training 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.

Security Function: Detect

Overview

Although NARA continues to enhance its implementation of various tools and processes to detect threats and vulnerabilities to improve its continuous monitoring program, much work remains to measure and evaluate this progress and its effectiveness. NARA has however made improvements in the security authorization and assessment process and related controls, and has developed, tailored and communicated an Information Security Continuous Monitoring (ISCM) strategy. As a result, NARA's Detect controls were upgraded to "Consistently Implemented" level of maturity.

Metric Domain – Information Security Continuous Monitoring

The goal of ISCM is to combat information security threats by maintaining ongoing awareness of information security, vulnerabilities, and threats to federal systems and information. ISCM provides ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness. In addition, specific requirements as defined within *NARA's Assessment & Authorization Handbook* and the NARA *Cybersecurity (CS) Handbook*, requires system owners to develop a strategy for continuous monitoring of the information system to include assessing all security controls, including common and hybrid controls, implemented at the system level to be assessed annually.

An integral part of information security continuous monitoring is the evaluation of security controls and authorizing a system to operate. However, we noted that NARA did not ensure a final approved ATO was in place for 2 of 10 sampled systems while in operation. Refer to the Risk Management domain section of this report for details related to this finding.

Recommendations:

For FISMA recommendations related to the weaknesses noted in the Information Security Continuous Monitoring domain refer to the Risk Management domain above.

Security Function: Respond

Overview

NARA has defined and communicated an updated enterprise level incident response plan, utilized several tools to provide 24/7 monitoring capability for the agency's network, and has agreements with third parties to provide technical assistance as needed.

Metric Domain – Incident Response

Information security incidents occur on a daily basis. Agencies must have comprehensive policies and planning in place to respond to these incidents and report them to the appropriate authorities. The United States Computer Emergency Readiness Team (US-CERT) is to receive reports of incidents on unclassified federal Government systems, and OMB requires the reporting of incidents that involve sensitive data, such as PII, within strict timelines.

NARA has defined and communicated its policies and procedures related to incident detection and analysis and has defined a common threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. However, NARA has open weaknesses[19] related to audit logging, and has indicated within their Incident Response Handbook, that they are implementing additional requirements for logging, log retention and log management based on Executive Order 14028, Section 8 *Improving the Federal Government's Investigative and Remediation Capabilities*, and ensuring those logs are collected centrally.

Recommendations:

No recommendations are being made for the Incident Response domain.

[19] *National Archives and Records Administration's Fiscal Year 2022 Federal Information Security Modernization Act of 2014 Audit*. OIG Report Number 22-AUD-09 (9/29/22), Recommendations #16, 19 and 20

Security Function: Recover

Overview

NARA has defined policies and procedures for developing, updating, and testing its contingency plans to ensure the program is consistently implemented across NARA.

Metric Domain – Contingency Planning

FISMA requires agencies to prepare for events that may affect an information resource's availability. This preparation requires identification of resources and risks to those resources, and the development of a plan to address the consequences if the loss of a system's availability occurs. Consideration of risk to an agency's mission and the possible magnitude of harm caused by a resource's unavailability are key to contingency planning.

NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, defines contingency planning as "interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods."

NARA has defined and communicated roles and responsibilities related to contingency planning and has consistently implemented those roles and responsibility across the organization, based upon a review of contingency planning exercises performed and associated roles and responsibilities. In addition, we noted that business impact analysis had been defined, were completed and current for all sampled systems. As a result, although NARA has consistently implemented contingency planning processes, they have not employed automated mechanisms to test system contingency plans more thoroughly and effectively.

Recommendations:

No recommendations are being made for the Contingency Planning domain.

Appendix A: Background

NARA Overview

NARA is an independent agency within the executive branch of the federal government responsible for preserving, protecting, and providing access to the records of our government. NARA has an FY 2023 appropriation request of 2,949 full time equivalents (FTEs) and budget request of $450 million.[20] NARA has a facility located in College Park, MD. NARA is directed by the Archivist who is appointed by President of the United States, with the advice and consent of the Senate. NARA's operations rely on 50[21] FISMA reportable information systems hosted both internally and externally. Total IT spending by NARA represents an annual investment of approximately $134 million.[22]

FISMA Legislation

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting federal operations and assets. FISMA requires federal agencies to develop, document, and implement an Agency-wide information security program and practices to protect their information and IT systems, including those provided or managed by another agency, contractor, or other source.

FISMA also provides a mechanism for improved oversight of federal agency information security programs and practices. FISMA requires agency heads to ensure:

(1) employees are sufficiently trained in their security responsibilities,
(2) a security incident response capability is established, and
(3) information security management processes are integrated with the agency's strategic and operational planning processes.

All agencies must also report annually to OMB and to Congressional committees on the effectiveness of their information security program and practices.

Federal agencies are to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency. As specified in FISMA, the agency CIO or senior official is responsible for overseeing the development and maintenance of security operations that continuously monitor and evaluate risks and threats.

FISMA also requires agency IGs to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB and by NIST (in its 800 series of Special Publications) supporting FISMA implementation. In addition, NIST issued the FIPS to establish agency baseline security requirements.

[20] https://www.archives.gov/files/about/plans-reports/performance-budget/2023-nara-congressional-justification.pdf.

[21] Based upon a master system inventory listing of all NARA operational FISMA reportable systems as of 1/06/2023.

[22] https://www.itdashboard.gov/itportfoliodashboard, National Archives and Records Administration – Information Technology Agency Summary.

IG FISMA Reporting Requirements

OMB and DHS annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On December 2, 2022, OMB issued Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*.[23] This memorandum described key changes to the methodology for conducting FISMA audits; and the processes for Federal agencies to report to OMB, and where applicable, DHS. Key changes to the methodology included:

- The OMB selected a core group of 20 metrics that IGs must evaluate annually and a selection of 20 Supplemental IG FISMA Reporting Metrics that must be evaluated during FY 2023.[24] The remainder of standards and controls will be evaluated on a two-year cycle.
- In previous years, IGs have been directed to utilize a mode-based scoring approach to assess maturity levels. In FY 2023, ratings were focused on calculated averages, wherein the average of the metrics in a particular domain would be used by IGs to determine the effectiveness of individual function areas (Identity, Protect, Detect, Respond, and Recover). IGs were encouraged to focus on the calculated averages of the 20 Core IG FISMA Reporting Metrics, as these tie directly to the Administration's priorities and other high-risk areas. In addition, OMB M-23-03 indicated that IGs should use the calculated averages of the Supplemental IG FISMA Reporting Metrics and progress addressing outstanding prior year recommendations as data points to support their risk-based determination of overall program and function level effectiveness. The calculated averages can be found in the FY 2023 IG FISMA Reporting Metrics, which was provided to the Agency separate from this report.

The FY 2023 IG FISMA Reporting Metrics provided the reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs and practices.

For this year's review, IGs were to assess the 20 Core and 20 Supplemental IG FISMA Reporting Metrics in the five security function areas to assess the maturity level and effectiveness of their agency's information security program and practices. As highlighted in **Table 3**, the IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and practices and align with the five functional areas in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover.

Table 3: Aligning the Cybersecurity Framework Security Functions to the FY 2023 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metric Domains
Identify	Risk Management and Supply Chain Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring

[23] M-23-03-FY23-FISMA-Guidance-2.pdf (whitehouse.gov) (December 2, 2022).
[24] https://www.cisa.gov/resources-tools/resources/fy23-24-ig-fisma-metrics.

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metric Domains
Respond	Incident Response
Recover	Contingency Planning

The foundational levels of the maturity model 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 strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy 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 strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Appendix B: Objective, Scope, and Methodology

Objective

The objective of this 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 DHS IG FISMA Reporting Metrics.

Scope

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

For this year's review, OMB required IGs to assess 20 Core and 20 Supplemental IG FISMA Reporting Metrics in five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security programs and practices and the maturity level of each function area. The maturity levels range from lowest to highest — Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

Consistent with FISMA and OMB requirements, our audit objective was to assess the effectiveness of NARA's information security program and practices in accordance with the FISMA of 2014, and applicable instructions from OMB and IG FISMA Reporting Metrics.

Our scope was to determine whether NARA implemented an effective information security program and practices for FY 2023. The effectiveness of the information security program and practices is defined as achieving a certain maturity level for each function area and domain based on the unique challenges of the organization.

For this audit, we reviewed select controls for a sample of 10 systems from a total population of 50 systems in NARA's FISMA inventory of information systems as of January 6, 2023.

In addition, we assessed NARA's technical controls by performing a vulnerability assessment and penetration test covering six of the 10 sampled systems. These tests included web facing applications and general support systems. The internal and external penetration tests were conducted to determine the effectiveness of controls that prevent or detect unauthorized access, disclosure, modification, or deletion of sensitive information. The results of the internal and external penetration tests were incorporated into our FISMA audit results.

In addition, the audit included an assessment of effectiveness for each of the nine FY 2023 IG FISMA Metric Domains and the maturity level of the five Cybersecurity Framework Security Functions. The audit also included a follow up on prior audit recommendations to determine if NARA made progress in implementing the recommended improvements concerning its information security program and practices. Refer to Appendix C for the status of prior-year recommendations.

We performed audit fieldwork which covered NARA's headquarters located in College Park, MD, from January 2023 to August 2023. The audit covered the period from October 2022 through August 2023.

Methodology

To accomplish the audit objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA.
- Reviewed documentation related to NARA's information security program and practices, such as security policies and procedures, system security plans, security control assessments, risk assessments, security assessment authorizations, plan of action and milestones, incident response plans, configuration management plans, and continuous monitoring plans.
- Tested system processes to determine the adequacy and effectiveness of selected controls. Testing procedures included penetration testing.
- Reviewed the status of recommendations in prior year FISMA reports, including supporting documentation to ascertain whether the actions taken addressed the noted weaknesses.

NARA's population of systems included 50 systems as of January 6, 2023, which were identified as a "Major Application" or "General Support System." Using a judgmental risk-based determination, we chose a representative sample size of 10 systems. Specifically, sample selection took into consideration the following: system was included within the scope of the FY 2023 NARA financial statement audit, was not planned to be decommissioned, was categorized as either a major application or general support system, covered a cross section of system owners and ISSOs, lines of business, whether it contained PII or not, and was primarily indicated as a moderate or high risk rated system.

In addition, we assessed NARA's technical controls by performing a vulnerability assessment and penetration test of six of the 10 sampled systems as part of the FISMA audit. We conducted internal (within the NARA network) and external (outside of the NARA network) vulnerability assessment and penetration testing to determine the effectiveness of technical controls. The results of the internal and external penetration tests were incorporated into our FISMA audit results.

In testing for the adequacy and effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered the relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population.

Our work in support of the audit was guided by applicable Agency policies and federal criteria, including, but not limited to, the following:

- Public Law 113-283, S.2521, December 18, 2014, *Federal Information Security Modernization Act of 2014*.
- *Government Auditing Standards* (April 2021).

- OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (December 2, 2022).
- *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (February 10, 2023).
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020 (includes updates as of December 10, 2020)).
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations* (January 2022).
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (December 2018).
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011).
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (April 16, 2018).
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003).
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* (September 2008).
- NIST SP 800-161, Revision 1*, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (May 2022).
- NIST FIPS 140-3, *Security Requirements for Cryptographic Modules* (March 22, 2019).
- OMB A-130, *Managing Information as a Strategic Resource* (July 28, 2016).
- OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– "Policy for a Common Identification Standard for Federal Employees and Contractors*" (February 3, 2011).
- OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* (May 21, 2019).
- Public Law 115-390, *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the "SECURE Technology Act"* (December 21, 2018).
- Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).
- Department of Homeland Security Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities* (November 3, 2021).

Appendix C: Current Year Status of Prior FISMA Report Recommendations

The following is the status of open recommendations from prior FISMA reports. The status of prior-year FISMA open recommendations was determined through a review of NARA's overall status of prior recommendations and testing the effectiveness of NARA's information security program and practices covering FY 2023. Based on these efforts we determined that 19 prior-year recommendations were closed, and 28 recommendations were determined still open as of August 2023.

Prior Years' FISMA Recommendations that Were Closed

Fiscal Year 2021, OIG Report Number 22-AUD-04 Audit of NARA's Compliance with FISMA	
Number	**Recommendation**
1	Ensure all systems have POA&Ms created when weaknesses are identified, to include completion dates; are remediated timely; and are updated to include detailed information on the status of corrective actions.
2	Ensure plans of actions and milestones are created, updated, remediated, and closed, for each system (including for 'failed' controls identified in Security Assessment Reports), in accordance with NARA policies, guidance and directives.
3	Ensure plans of actions and milestones for the NARANet and OFAS systems are created, updated and remediated, for each system, in accordance with NARA policies, guidance and directives, to include enhanced POA&M closure procedures.
4	Ensure inconsistencies described regarding the POA&M closure process stated within and between the Cybersecurity Framework Methodology (CFM), NARA IT Security Methodology for Certification and Accreditation (CA) and Security Assessments, and the NARA ISSO Guide are identified and resolved.
10	Ensure individual system security plans are revised (as needed) to reflect the changes made to the standard data elements/taxonomy for hardware inventories, within the CFM.
12	Upon completion of the FY 2021 annual laptop asset inventory and the reconciliation of any discrepancies, update NARA asset management policies and procedures to reflect lessons learned to improve the accuracy, completeness, and timeliness of NARA's asset inventory process.
24	Ensure system owners and ISSOs have completed an E-Authentication Threshold Analysis (ETA) for all information systems, with a signed E-Authentication Risk Assessment (if required).
25	Review and reduce the number of NARA users assigned to the PIV debarment group and move to the PIV Mandatory group, using a risk-based decision process.
30	Ensure account reviews are completed in accordance with Access Control IT Methodology requirements.

Fiscal Year 2022, OIG Report Number 22-AUD-09
Audit of NARA's Compliance with FISMA

Number	Recommendation
2	Identify all FISMA reportable systems in which the Authorizing Official (AO) listed within the ATO, has subsequently changed.
3	For those systems identified in which the AO listed in the ATO has changed, follow the NARA Security Methodology for Certification and Accreditation and Security Assessment in regard to requirements upon changes in AO. This is a separate activity from the ongoing authorization process.
4	Update the CFM for ongoing authorizations, to include examples of situations where a change in status could prompt the independent security control assessor to recommend re-certification of a system.
5	Continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include but are not limited to those systems identified in which the AO listed in the ATO has changed, NARA should follow the NARA Security Methodology for Certification and Accreditation (C&A) and Security Assessments regarding requirements upon changes in AOs. This is a separate activity from ongoing authorization processes.
7	Develop and implement formalized procedures to ensure for those systems utilized by NARA and managed by Cloud Service Providers, controls for which NARA has a shared responsibility should be reviewed on an annual basis, documented, and assessed as to the impact to NARA of any risks that may be present.
8	● Require that providers of external information system services comply with NARA information security requirements, ● Define and document government oversight and user roles and responsibilities with regard to external information systems, and ● Establish a process to monitor security control compliance by external service providers on an ongoing basis.
9	Add an addendum to current agreements which requires compliance with NARA's information security requirements.
10	Conduct risk assessments for each system in operation and establish policies or procedures to ensure that risk assessments are conducted at least annually.
24	Coordinate with system owners and ISSOs, identify and remediate inconsistencies in contingency plan testing requirements between the CFM and the NARA IT Security Methodology for Contingency Planning to ensure requirements are more clearly defined and consistently communicated. As needed, NARA will then update contingency plan testing to be commensurate with the availability risk level assigned.
25	Identify and remediate inconsistencies in contingency plan testing requirements between the CFM and the NARA IT Security Methodology for Contingency Planning, to ensure requirements are more clearly defined and consistently communicated. As needed, NARA will then update contingency plan testing to be commensurate with the availability risk level assigned.

Prior Years' FISMA Recommendations that Remain Open

Note: *These remaining open recommendations do not represent and are not intended to represent all recommendations which were closed within the respective years or reports identified.*

Fiscal Year 2021, OIG Report Number 22-AUD-04 Audit of NARA's Compliance with FISMA	
Number	**Recommendation**
13	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.
14	Develop and communicate an organization wide Supply Chain Risk Management strategy and implementation plan to guide and govern supply chain risks.
15	Document and implement a process to track and remediate persistent configuration vulnerabilities or document acceptance of the associated risks.
16	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.
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.
18	Fully complete the migration of applications to vendor supported operating systems.
22	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.
26	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.
27	Enforce mandatory PIV card authentication for all NARANet users, in accordance with OMB requirements.
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.
29	Ensure NARANet user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements.
33	The SAOP review and update the "NARA 1609 Initial Privacy Reviews and Privacy Impact Assessments" privacy policies and procedures to reflect NARA's current processes and controls.
34	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, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements.

Fiscal Year 2022, OIG Report Number 22-AUD-09 ***Audit of NARA's Compliance with FISMA***	
Number	**Recommendation**
1	Ensure complete security authorization packages for each major application and general support system is completed prior to deployment into production.
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.
11	Ensure IT policies, procedures, methodologies, and supplements are reviewed and approved in accordance with NARA Directive 111.
12	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
13	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.
14	Ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported.
15	Document, communicate and implement NARA's configuration management processes applicable to all NARA systems, not just those under ECAB control, within NARA's Configuration Management (CM) program management plan or other NARA methodology.
16	Implement the following corrective actions: ● Complete efforts to implement the Security Information 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, and ● Ensure the procurement of new IT system hardware and software, which provides user authentication, includes a minimum set of audit logging.
17	Ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy.
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."
19	Ensure audit logging is enabled for each major information system.
20	Ensure periodic reviews of generated audit logs are performed for each major information system.
21	Ensure password configuration settings for all major information systems are in accordance with NARA IT Security Requirements.
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.
23	Ensure a process is developed, documented, and implemented to change passwords whenever users within shared/group accounts change.

Appendix D: Acronyms

AO	Authorizing Official
ATO	Authorization to Operate
CFM	Cybersecurity Framework Methodology
CIO	Chief Information Officer
CLA	CliftonLarsonAllen LLP
CM	Configuration Management
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DNS	Domain Name Service
ECAB	Enterprise Change Advisory Board
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
ICAM	Identity, Credentialing and Access Management
IG	Inspectors General
IT	Information Technology
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plans of Actions and Milestones
RMF	Risk Management Framework
SA&A	Security Assessment and Authorization
SAOP	Senior Agency Official for Privacy
SCRM	Supply Chain Risk Management
SOP	Standard Operating Procedure
SP	Special Publication

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

Chief Operating Officer

General Counsel

Deputy Chief Operating Officer

Chief of Management and Administration

Chief Information Officer

Accountability

General Accountability Office

United States House Committee on Oversight and Government Reform

Senate Homeland Security and Government Affairs Committee

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 and letters to the Hotline post office box, we also accept emails through an online referral form. Walk-ins are always welcome. Visit *www.archives.gov/oig/* for more information, or contact us:

By telephone
Washington, DC, Metro area: 301-837-3500
Toll-free: 800-786-2551

By mail
NARA OIG Hotline
P.O. Box 1821
Hyattsville, MD 20788-0821

By facsimile
301-837-3197

By online referral form
www.archives.gov/oig/referral-form/index.html