NATIONAL ARCHIVES | Inspector General

September 29, 2022

TO: Debra Steidel Wall
Acting Archivist of the United States

FROM: Dr. Brett M. Baker
Inspector General

SUBJECT: *National Archives and Records Administration's Fiscal Year 2022 Federal Information Security Modernization Act of 2014 Audit*
OIG Report No. 22-AUD-09

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 2022.

CLA is responsible for the attached auditor's report dated September 29, 2022 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.

Results of the Independent Audit
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." Specifically, the six functional areas achieved a maturity level of "Defined" (Level 2) for an overall maturity level of "Defined" for the security program. While NARA's overall maturity level has not changed from last year, notable this year was decreased maturation of Identity and Access Management from the "Defined" level to "Ad Hoc." In addition, five domains were assessed at the "Defined" level (Risk Management, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning) and three domains at the "Ad Hoc" level (Supply Chain Risk Management, Configuration Management, and Data Protection and Privacy).

The report contains one new recommendation and 24 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. In addition, we noted 9 recommendations related to prior FISMA audits were closed.

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 or Jewel Butler, Assistant Inspector General for Audits, with any questions.

Attachment

cc: Micah Cheatham, Chief of Management and Administration
William Bosanko, Chief Operating Officer
Sheena Burrell, Chief Information Officer
Gary M. Stern, General Counsel
Meghan Guthorn, Deputy Chief Operating Officer
Kimm Richards, Accountability
Jewel Butler, Assistant Inspector General for Audits
Carol Seubert, Senior Financial Auditor
Andrew Clements, Senior IT 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 2022
Federal Information Security Modernization Act of 2014 Audit

Final Report

September 29, 2022

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203

phone 571-227-9500 **fax** 571-227-9552
CLAconnect.com

September 29, 2022

Brett Baker
Inspector General
National Archives and Records Administration
Office of the Inspector General
8601 Adelphi Road
College Park, MD 20740

Dear Dr. Baker:

CliftonLarsonAllen LLP is pleased to present our performance audit report on 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 for fiscal year 2022.

We appreciate the assistance we received from NARA. We would be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

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) 2022. 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 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 in accordance with FISMA and applicable instructions from OMB and the Department of Homeland Security (DHS) IG FISMA Reporting Metrics.

For FY 2022, OMB required IGs to assess 20 Core IG Metrics in five security function areas – Identify, Protect, Detect, Respond, and Recover – to determine the effectiveness of their agencies' information security programs and the maturity level of each function area. The maturity levels are Level 1 - Ad Hoc, Level 2 - Defined, Level 3 - Consistently Implemented, Level 4 - Managed and Measurable, and Level 5 - Optimized. To be considered effective, an agency's information security program must be rated Level 4 – Managed and Measurable or above.

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 2022 FISMA Core IG 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 51 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 April 2022 to August 2022. The audit covered the period from October 1, 2021 through August 15, 2022.

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 was "Not Effective." Specifically, four functional areas (Identify, Detect, Respond and Recover) achieved a maturity level of "Defined" (Level 2) and one functional area (Protect) achieved a maturity level of "Ad Hoc" for an overall maturity level of "Defined" for the security program. NARA's overall maturity level has not changed from last year, with eight of nine domains remaining at the same maturity level as last year (Risk Management, Supply Chain Risk Management, Configuration Management, Data Protection and Privacy, Security Training, 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.

We made one new recommendation and included within the body of the report 24 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. In addition, we noted 18 recommendations related to prior FISMA audits are still open which have not missed their target completion date, and 9 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 September 29, 2022. We have no obligation to update our report or to revise the information contained herein to reflect events occurring after September 29, 2022.

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

Arlington, Virginia
September 29, 2022

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
2022 FISMA AUDIT

Table of Contents

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 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 Agency information security programs and practices. 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 an audit in support of the FISMA requirement for an annual audit of NARA's information security program and practices. 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 (the Core IG FISMA metrics).[2]

To address FY 2022 Core IG FISMA 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 scope and methodology. We also reviewed the status of the 51 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.

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 was "Not Effective." Specifically, four functional areas (Identify, Detect, Respond and Recover) achieved a maturity level of "Defined" (Level 2) and one functional area (Protect) achieved a maturity level of "Ad Hoc" for an overall maturity level of "Defined" for the security program. 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.

NARA's information security program has longstanding weaknesses in developing and consistently implementing policies and procedures. Although NARA relies heavily on the *Cybersecurity Framework Methodology* (CFM) as its documented policy for meeting FISMA requirements, it does not accurately reflect the current state of NARA's information security program in many cases. In addition, controls need to be applied in a comprehensive manner to

[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 Agency of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] We submitted our responses to the FY 2022 IG FISMA Core Metrics to NARA OIG as a separate deliverable under the contract for this performance audit.

information systems across NARA to be considered consistent and fully effective by achieving at least a rating of Level 4, "Managed and Measurable."

We made one new recommendation and included within the body of the report 24 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. In addition, we noted 18 recommendations related to prior FISMA audits are still open which have not missed their target completion date, and 9 recommendations were closed.

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, 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 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 2022 IG Cybersecurity Framework Function and Domain Ratings

Cybersecurity Framework Security Functions[3]	FY 2022 Maturity Level by Function	Metric Domains	Domain Maturity Level	Change from FY 2021
Identify	Defined (Level 2)	**Risk Management**	Defined (Level 2)	No Change
		Supply Chain Risk Management	Ad Hoc (Level 1)	No Change[4]
Protect	Ad Hoc (Level 1)	**Configuration Management**	Ad Hoc (Level 1)	No Change
		Identity and Access Management	Ad Hoc (Level 1)	Downgraded from Defined (Level 2)
		Data Protection and Privacy	Ad Hoc (Level 1)	No Change
		Security Training	Defined (Level 2)	No Change

[3] 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.
[4] This domain was not considered in the Identify framework function rating for FY 2021.

Cybersecurity Framework Security Functions[3]	FY 2022 Maturity Level by Function	Metric Domains	Domain Maturity Level	Change from FY 2021
Detect	Defined (Level 2)	**Information Security Continuous Monitoring**	Defined (Level 2)	No Change
Respond	Defined (Level 2)	**Incident Response**	Defined (Level 2)	No Change
Recover	Defined (Level 2)	**Contingency Planning**	Defined (Level 2)	No Change
Overall	**Level 2: Defined - Not Effective**			

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 and account management controls. Specifically, NARA continued its progress toward a more mature information security program, including the following:

- Information Services continues with updates to their security methodologies and IT security handbooks.
- A configuration management plan template was developed to include security baselines and baseline deviation processes, with template rollouts ongoing for FISMA reportable systems.
- Improvements were made in the process of disabling privileged user network accounts in which individuals had not completed their annual Tier II Cyber Security/Personally Identifiable Information (PII) training in a timely manner.
- Improvements were made with documentation of system controls within information system security plans and the assignment of Information System Security Officers.

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. Additionally, NARA needs to ensure:

- The security assessment and authorization packages are completed and updated timely.
- Information security weaknesses are more consistently documented, monitored, and closed.
- Multi factor authentication is enforced agency wide.
- Configuration management plans and policies and procedures are either developed or enhanced.
- 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.
- Hardware asset inventories are more effectively managed.
- Contingency plan testing and requirements noted within policies and procedures are in alignment.

NARA's information security program has longstanding weaknesses in developing and consistently implementing policies and procedures. Although NARA relies heavily on the CFM as its documented policy for meeting FISMA requirements, it does not accurately reflect the current state of NARA's information security program in many cases. Specifically, there continues to be no consistency or completeness of and between the CFM and other NARA policies and procedures, including the Information Technology (IT) security architecture and methodology documents, the *Information System Security Officer (ISSO) Guide*, and individual system security documentation, describing IT security policies and procedures. Examples of inconsistencies include the extent of contingency plan testing required for an information system, when a system should be re-authorized, and who is responsible for the approval and closure of plans of actions and milestones.

These conflicting requirements and guidance result in an inconsistent implementation and communication of security controls throughout the agency. Since the Core IG FISMA metrics require sound policies and procedures at the foundational levels for the maturity model, the weaknesses found in NARA's development, implementation, and communication of policies and procedures resulted in the agency continuing to receive "Ad Hoc" maturity levels for several of the metric domains.

Highlights of key observations pertaining to policies and procedures include the following:

- When a change in Authorizing Official (AO) occurred, NARA did not document the new AO acknowledgement of the risks to current systems.
- Contingency plans were inconsistently tested due to conflicting requirements within the CFM and other policy and procedure documents.

In order to demonstrate measurable improvements towards an effective information security program, 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,[5] with 42 recommendations remaining open, we made 1 new recommendation to help NARA address challenges in its development of a mature and effective information security program.

Table 2: Weaknesses Noted in FY 2022 FISMA Audit Mapped to Domains in the FY 2022 Core IG FISMA Metrics

FY 2022 Core IG FISMA Metric Domains	Weaknesses Noted
Risk Management	Security Assessment and Authorization (SA&A) documentation was not reviewed when there was a change in AO, controls were not tested, or security documentation was incomplete.
	System hardware inventories were incomplete or not properly managed.

[5] FY 2021 "*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).

FY 2022 Core IG FISMA Metric Domains	Weaknesses Noted
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.
	E-Authentication Risk Assessments (or E-Authentication Risk Analysis) were not always completed.
	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	The annual continuous monitoring of information security controls was not performed consistently for all systems.
Security Training	Prior-year weaknesses remained open related to specialized role-based training.
Contingency Planning	NARA did not perform contingency plan testing commensurate with the availability risk of the information system.

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 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 report distribution list.

FISMA Audit Findings
Security Function: Identify

Overview

NARA developed and published the CFM 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. Specifically, we identified weaknesses related to SA&A documentation, which was not properly approved, and security documentation was outdated or did not exist. In addition, NARA's asset management practices and controls, specific to the maintenance of hardware assets, were determined to not be accurate or consistently implemented.

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[6] 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. In addition, NARA policy[7] states that in the event of a change in AO, the new AO should review the current authorization decision document, authorization package, and any updated documents created because of ongoing monitoring activities. If the new AO is willing to accept the currently documented risk, then they would sign a new authorization decision document. This process

[6] NARA Cyber Security Framework Methodology Processes & Procedures, v1.16, 9/01/2021.
[7] NARA IT Security Methodology for Certification and Accreditation and Security Assessment, 9/16/2021, version 7.7.

would formally transfer responsibility and accountability for the information system, or the common controls inherited by organizational information systems and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation.

As a result of system owners not effectively managing their systems and complying with NARA policies, for the sample of NARA systems within scope, we noted the following weaknesses in the management of NARA's security assessment and authorization process:

- For 3 of 10 sampled systems, although the AO listed within the Authorization to Operate (ATO), has subsequently changed from the former Chief Information Officer (CIO)/Assistant Archivist for Information Services to the new CIO, a new authorization decision document has not been signed to indicate the new AO (new CIO) is willing to accept the documented risk.

  NARA has indicated an action plan to address this weakness is in progress and is expected to be addressed within IT Security Handbooks which are under development; however, these actions are not expected to be completed until September 30, 2022.

- We noted that 1 of 10 sampled systems, has been in operation since 2015 without a complete Security Authorization package to include an ATO, security assessment report, risk assessment report, or security certification recommendation. Thus, the system owner has not ensured that a security authorization package was developed and approved since 2015.

- For 1 of 10 sampled systems, although an ATO was provided, it was not completed until June 2022. Thus, the ATO was not in place for a significant portion (9 months) of FY 2022. NARA had indicated that this system was under a state of continuous authorization and monitoring, during the interim period.

In addition to system owners not effectively managing their systems and complying with NARA policies, these weaknesses were also attributed to a lack of clarity within NARA's CFM related to Ongoing Authorizations and what constitutes a "change in status" for recertification, along with ongoing policy updates and clarifications. As a result, system re-certification efforts were not being performed upon a change an AO.

In addition, delays in the assignment of ISSOs to some systems have delayed the development of requisite security documentation, the subsequent performance of the security assessment phase, and preparation of authorization packages.

Without documented evidence the current AO explicitly accepts the risks of a system they are responsible for, it is unknown whether a transfer of responsibility and accountability for the information system or the common controls inherited by the information system has occurred. Also, without the performance of an annual security control assessment of an information system, there is a risk that high or critical weaknesses could exist and not be detected or remediated in a timely manner.

Asset Inventory

NIST standards[8] require NARA to develop and document a comprehensive inventory of information system components that accurately reflects the current information systems including all components within the authorization boundary of the system which is at the level of granularity deemed necessary for tracking and reporting.

NARA's asset management practices and controls, specific to the maintenance of hardware assets, were not accurate or consistently implemented. Weaknesses were noted in the content and taxonomy of hardware inventory listings.

Although the CFM defines standard data elements/taxonomy for the inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting, the standard taxonomy was not consistently implemented throughout the fiscal year. Specifically, for 1 of 10 sampled systems, the hardware asset inventory was not complete and was missing certain attributes as required within the CFM.[9] Due to inconsistent policies and procedures related to the content of hardware inventories, these inventories did not always include required content.

Additionally, NARAs asset management policies and procedures were not effectively implemented. Specifically, we noted NARA has not completed a physical asset inventory of laptops, desktops, and printers since 2019, when it transitioned to a new asset management software. The inventory is used to reconcile and validate whether all assets were accurately and completely stated. NARA management indicated a physical inventory is in process; however, this effort is not expected to be completed until September 2022.

The implementation of the annual physical inventory count for FY 2022 was unable to be completed due to Coronavirus Disease (COVID-19) restrictions over the past 2 years, due to contractor resource issues, and a planned transition to a new contractor.

Without up-to-date inventories, there is an increased risk that assets may not be tracked and reported, and potentially not secured and protected.

Recommendations:

We recommend the NARA CIO take the following actions to address prior unimplemented recommendations related to the weaknesses noted for the Risk Management domain:[10]

1. Ensure complete security authorization packages for each major application and general support system is completed prior to deployment into production. (Recommendation #1 from FY2018 FISMA audit, report #19-AUD-02)

2. Identify all FISMA reportable systems in which the AO listed within the ATO, has subsequently changed. (Recommendation #5 from FY2021 FISMA audit, report #22-AUD-04)

[8] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, security control, CM-8 Information System Component Inventory.
[9] *Cybersecurity Framework Methodology* (Section 2.2.1 Information System Component Inventory pg. 21).
[10] 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.

3. For those systems identified in which the AO listed in the ATO has changed, NARA should 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. (Recommendation #6 from FY2021 FISMA audit, report #22-AUD-04)

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. (Recommendation #7 from FY2021 FISMA audit, report #22-AUD-04)

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. (Recommendation #12 from the FY2021 Financial audit, report #22-AUD-02)

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. (Recommendation #11 from FY2021 FISMA audit, report #22-AUD-04)

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. (Recommendation #1 from FY2015 FISMA audit, report #16-02)

8. For future agreements, the CIO should:
    - 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. (Recommendation #13 from the FY2015 FISMA audit, report #16-02)

9. Add an addendum to current agreements which requires compliance with NARA's information security requirements. (Recommendation #14 from the FY2015 FISMA audit, report #16-02)

10. Conduct risk assessments for each system in operation and establish policies or procedures to ensure that risk assessments are conducted at least annually. (Recommendation #4 from the FY2018 FISMA audit, report #19-AUD-02)

11. Ensure IT policies, procedures, methodologies, and supplements are reviewed and approved in accordance with NARA Directive 111. (Recommendation #8 from the FY2018 FISMA audit, report #19-AUD-02)

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 – 115th, 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 reported in last year's FISMA audit,[11] 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 been completed, as NARA continues to evaluate guidance provided by NIST in 800-161, Revision 1, Cybersecurity *Supply Chain Risk Management Practices for Systems and Organizations*, released in May 2022 and based on Executive Order 14028 (*Executive Order on Improving the Nation's Cybersecurity)*.

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.[12]

[11] FY 2021 "*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.

[12] 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 2022. See Appendix C for status of prior recommendations, organized by FY 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 2022, 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, a comprehensive enterprise-wide configuration management information security policy does not exist, configuration management plans were not developed for all systems, and configuration and patching weaknesses continue.

Vulnerability Management Program

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, security control System and Information Integrity, Flaw Remediation SI-2, 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, Vulnerability Monitoring and Scanning RA-5, 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 2021 and before. Due to the vulnerabilities identified, the assessment team was able to exploit certain vulnerabilities.

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. In addition, some NARA websites did not have Cross-site Request Forgery tokens consistently implemented.

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.

In addition, we noted the following unresolved prior-year weaknesses[13] which included:

- NARA not having an organization wide deviation process that incorporates all Change Control Boards, and;
- processes for approvals or deviations from configuration baselines were still under development.

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 recommendations related to the weaknesses noted for the Configuration Management domain:

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. (New Recommendation)

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. (Recommendation #12 from the FY2018 FISMA audit, report #19-AUD-02)

14. Ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported. (Recommendation #13 from the FY2018 FISMA audit, report #19-AUD-02)

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. (Recommendation #21 from the FY2021 FISMA audit, report #22-AUD-04)

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

[13] FY 2021 "*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 #21.

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[14] 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[15] states Agencies shall require PIV credentials (where applicable in accordance with OPM 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 the following information security weaknesses related to PIV authentication:

- An E-Authentication Risk Assessment (or E-Authentication Risk Analysis) was not completed for 7 of 10 sampled systems, in accordance with the CFM, section 3.14.4. In addition, the specific requirement for ISSO's to perform E-Authentication risk assessments or analysis is not described within the ISSO Guide.

  NARA has indicated they have completed a review of federal guidance related to Digital Identity Risk Assessment which will be incorporated into the IT Security handbook being developed, along with accompanying templates to be completed, however these efforts are not anticipated to be completed until September 2023.

- The use of PIV or other form of multi factor authentication for privileged and non-privileged user access to the network is not currently mandatory or required. Although there is a requirement for employees to access NARA equipment and the network using two-factor authentication, an option exists for network access via password authentication, where two-factor authentication is not mandatory for those users placed into a "debarment group."[16] Of the 164 users with blanket assignment to the "permanent debarment group", about 163 are planned to be moved back to the "PIV Mandatory" group.

- The CFM, section 3.14.1 indicates that NARA users (both privileged and non-privileged) have the option to log into their workstations with their PIV cards, but since it is not mandatory, this is not in accordance with OMB Memorandum M-11-11 and M-19-17 requirements. NARA has indicated they are determining necessary funding requirements to facilitate requiring PIV for all privileged users and to implement PIV at the server level for all applications.

Although the CFM requires ISSOs to conduct an E-Authentication Risk Assessment, this specific requirement is not addressed within the NARA ISSO guide, resulting in this specific control not being consistently applied by the ISSOs.

In addition, the ongoing pandemic and related physical access restrictions, precluded some NARA employees and contractors from obtaining a PIV card, which resulted in NARA placing a

[14] OMB Memorandum M-11-11, *Continued Implementation Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractors*.
[15] OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential and Access Management*.
[16] The "debarment group" represents those user accounts which are not required to authenticate to the network using a PIV card.

large number of individuals into the PIV debarment group so they could authenticate into the network. As new PIV enabled laptops are deployed, PIV authentication requirements are expected to be enabled resulting in the removal of additional users from the debarment group, which is an ongoing process.

NARA is still completing the migration of an identity security and access management tool to require PIV authentication for all privileged users, servers, and applications. However, this effort is not expected to be completed until December 2022.

Without an e-authentication risk assessment or analysis, it may not be clear which e-authentication assurance level is applicable for a system and which respective identity proofing controls are required. In addition, authentication controls may not be appropriately tailored given a system's FIPS 199 risk rating and this may result in this specific control not being consistently applied by the ISSOs.

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

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 (CDM) requirements; incorporate applicable federal policies, standards, playbooks, and guidelines; and include roles and responsibilities for all users.

Specifically, we noted the following weaknesses related to ICAM:

- As reported in the NARA FY 2021 FISMA audit,[17] NARA had not developed a comprehensive ICAM policy or strategy which includes the establishment of related SOPs; identification of stakeholders; communicating relevant goals, task assignments, and measures; and reporting progress.

Although NARA has developed an ICAM Executive Board Charter which was signed by the Archivist, as of April 2022 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.

NARA has defined its process for provisioning, managing, and reviewing privileged accounts within the CFM and the Access Control Methodology. However, previously reported weaknesses related to account management controls including 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.

[17] FY 2021 "*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 #28.

Recommendations:

We recommend the NARA CIO take the following actions to address prior unimplemented recommendations related to the weaknesses noted for the Identity and Access Management domain.[18]

16. The CIO should implement the following corrective actions:
    - Complete efforts to implement the Net IQ Sentinel 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. (Recommendation #20 from the FY2015 FISMA audit, report #16-02)

17. Ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy. (Recommendation #15 from the FY2018 FISMA audit, report #19-AUD-02)

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." (Recommendation #16 from the FY2018 FISMA audit, report #19-AUD-02)

19. Ensure audit logging is enabled for each major information system. (Recommendation #20 from the FY2018 FISMA audit, report #19-AUD-02)

20. Ensure periodic reviews of generated audit logs are performed for each major information system. (Recommendation #21 from the FY2018 FISMA audit, report #19-AUD-02)

21. Ensure password configuration settings for all major information systems are in accordance with NARA IT Security Requirements. (Recommendation #22 from the FY2018 FISMA audit, report #19-AUD-02)

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. (Recommendation #23 from the FY2018 FISMA audit, report #19-AUD-02)

23. Ensure a process is developed, documented, and implemented to change passwords whenever users within shared/group accounts change. (Recommendation #24 from the FY2018 FISMA audit, report #19-AUD-02)

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 PII collected, used, maintained, shared, and disposed of by

[18] No new recommendations were noted for the Identity and Access Management domain. 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 Identity and Access Management domain. See Appendix C for status of prior recommendations.

information systems. Also, per Executive Order 14028, agencies are required to limit the transference of data by removable media.

NARA has not sufficiently defined its policies and procedures for areas including limiting the transfer of sensitive data to removable media. Although NARA employs various preventative and detective measures for data exfiltration and network defenses, the CFM 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. These weaknesses were attributed to the fact NARA plans and efforts to strengthen exfiltration and Data Loss Prevention (DLP) capabilities are still in progress.[19]

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[20] related to role-based privacy training for all individuals having responsibility for PII and privacy policies and procedure updates remained open during FY 2022.

Recommendations:

No recommendations are being made for the Data Protection and Privacy domain.[21]

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, 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[22] 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.[23]

[19] As indicated within NARA's Federal Managers Financial Integrity Act action plan for IT security weaknesses in April 2022.

[20] FY 2021 "*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.

[21] No recommendations were noted for the Data Protection and Privacy domain since 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.

[22] FY 2021 "*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.

[23] 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. As a result, NARA's Detect controls remain at the "Defined" level of maturity due to the inconsistent application of controls throughout NARA.

Metric Domain – Information Security Continuous Monitoring

The goal of Information Security Continuous Monitoring (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 CFM require 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. However, we noted that NARA did not document the new AO acknowledgment of the risks to current systems when a change in AO occurred, or an ATO was not in place for a system during the entire audit period. In addition, not all systems had a completed annual security control assessment.

Refer to authorization and accreditation, system security plan, and security control assessment weaknesses noted within the Risk Management domain section of this report which are related to ISCM.

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's incident response plan which includes roles and responsibilities for the timely reporting and handling of incidents has been defined and communicated. NARA has also defined processes to eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations; and demonstrated through sampled incident tickets how potential malware was contained and eradicated. However, it was not clear whether lessons learned were being captured and resulted in plan updates. Also, based upon sampled incident documentation provided, it was not clear whether NARA consistently utilized its defined threat vector taxonomy to classify incidents to demonstrate a consistently implemented maturity level.

Recommendations:

No recommendations are being made for the Incident Response domain.[24]

[24] No recommendations were made for the Incident Response domain since the weakness identified was more related to a clarification issue than an internal control weakness.

Security Function: Recover

Overview

NARA has defined policies and procedures for developing, updating, and testing its contingency plans; however, weaknesses remain affecting the effectiveness of controls 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 not consistently implemented contingency planning processes; thus, has not reached a level of maturity as defined by Core IG FISMA metrics to be an effective overall program.[25] For 9 of 10 sampled systems, we found contingency plans were not appropriately tested.

Although the NARA CFM indicates that functional tests will be performed for those systems with a "Moderate" or "High" risk availability rating, there were inconsistencies regarding contingency plan testing requirements when compared to other NARA policies and procedures, such as the *NARA IT Security Methodology for Contingency Planning*. This document states the system owner and ISSO are provided discretion as to the extent of testing to be performed. This testing can be contingent upon the availability level as stated in the System Security Plan (SSP) and Recovery Time Objectives (RTO), alternate site availability, and Business Continuity Strategy as determined by the system's Business Impact Analysis (BIA). This resulted in individuals not performing testing in a consistent manner and with sufficient rigor reflecting the information systems availability risk rating.

Specifically, we noted that 9 of 10 sampled systems had "tabletop exercises" performed as their annual contingency plan test. However, given their assigned FIPS 199[26] Availability rating of either "High" or "Moderate," contingency plan testing should have been "functional exercises," as required by NARA's CFM, specifically Section 6.5.3, Test, Training and Evaluations (TT&E) Program Summary, for "Moderate impact" and "High impact" systems.

Although these exercises were completed annually, a "tabletop" exercise is discussion based only, and does not permit personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. This occurred due to an ongoing

[25] A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable*.
[26] FIPS 199 – Federal Information Processing Standards – Standards for the Security Categorization of Federal Information and Information Systems. This document provides standards for categorizing information and information systems to provide appropriate levels of information security according to a range of risk levels, recommend types of information and information systems to be included in each category and provide minimum information security requirements in each such category.

policy clarification, as NARA's requirements for contingency plan testing were inconsistent and subject to interpretation.

Without the performance of contingency plan testing commensurate with the availability risk level of a system, there is an increased risk that in the event of a disaster, NARA may not be able to successfully execute recovery procedures and recovery time objectives may not be achieved.

Recommendations:

We recommend the NARA CIO take the following actions to address prior unimplemented recommendations related to the weaknesses noted for the Contingency Planning domain.

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. (Recommendation #35 from FY2021 FISMA audit, report #22-AUD-04)

25. In coordination 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. (Recommendation #21 from FY2021 Financial Statement audit, report #22-AUD-02)

Appendix A: Background

NARA Overview

NARA is an independent agency within the executive branch of the federal government responsible for openness, cultivating public participation, and strengthening our nation's democracy through public access to high-value government records. Public access to government records strengthens democracy by allowing Americans to claim their rights of citizenship, hold their government accountable, and understand their history so they can participate more effectively in their government.

NARA is directed by the Archivist who is appointed by President of the United States, with the advice and consent of the Senate. The Archivist is appointed without regard to political affiliations and solely based on the professional qualifications required to perform the duties and responsibilities of the office of Archivist.

NARA is structured with four main offices under the Archivist, which are the Office of Chief of Staff, Office of Chief of Operating Officer, Office of the Chief Management and Administration, and Office of Innovation. The Office of Chief Management and Administration oversees the Office of Chief of Financial Officer, Office of Chief Acquisition Officer, Information Services, Business Support Services, and Office of Human Capital. The Office of Chief Operating Officer oversees the Agency Services, Research Services, Office of the Federal Register, and Legislative Archives, Presidential Libraries, and Museum Services.

NARA's operations rely on 50[27] FISMA reportable information systems hosted both internally and externally. Total IT spending by NARA represents an annual investment of approximately $126.9 million.[28]

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 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. 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.

[27] Based upon a master system inventory listing of all NARA operational FISMA reportable systems as of 1/25/2022.
[28] https://viz.ogp-mgmt.fcs.gsa.gov/itportfoliodashboard, National Archives and Records Administration – Information Technology Agency Summary.

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.

FY 2022 Core IG FISMA Reporting Metrics

OMB and DHS annually provide instructions to federal agencies and IGs for preparing FISMA reports. On December 6, 2021, OMB issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*.[29] This memorandum describes 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:

- Selection of a core group of 20 metrics and highly valuable controls that must be evaluated annually. The remainder of standards and controls will be evaluated on a two-year cycle.
- OMB shifted the due date of the IG FISMA Reporting Metrics from October to July to better align with the release of the President's Budget.
- Use of this reporting timeline began in FY 2022 starting with the Core IG FISMA metrics.

The FY 2022 Core IG FISMA Reporting Metrics provided the reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs. For this year's review, IGs were to assess 20 Core IG FISMA Metrics in five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security program and the maturity level of each function area. The five function areas are supported by nine metric domain areas. The Core IG FISMA Metrics are designed to assess the maturity of the information security program 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, as highlighted in **Table 3**.

Table 3: Aligning the Cybersecurity Framework Security Functions to the FY 2022 Core IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2022 Core 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
Respond	Incident Response
Recover	Contingency Planning

[29] Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (whitehouse.gov)

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** 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: Scope and Methodology

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 IG FISMA metrics in five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security program 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 in accordance with the FISMA of 2014, and applicable instructions from OMB and DHS IG FISMA Reporting Metrics.

Our scope was to determine whether NARA implemented an effective information security program and practices for FY 2022. The effectiveness of the information security program 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 25, 2022.

In addition, the audit included an assessment of effectiveness for each of the nine FY 2022 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 April 2022 to August 2022. Given accelerated IG FISMA Metric reporting deadlines for FY 2022, the audit covered the period from October 1, 2021 through August 15, 2022.

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, such as security policies and procedures, system security plans, security control assessments, risk assessments, security assessment authorizations, plan of action and milestones, incident response plan, configuration management plan, continuous monitoring plan, and contingency planning documentation.

- Tested system processes to determine the adequacy and effectiveness of selected controls. Testing procedures included vulnerability assessment and penetration testing.
- Reviewed the status of recommendations in the prior year FISMA report, including supporting documentation to ascertain whether the actions taken addressed the noted weaknesses.

NARA's population of systems includes 50 systems as of January 25, 2022, 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 2022 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 an 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.

To perform our audit of NARA's information security program and practices, we followed a work plan based on the following guidance:

- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*.
- OMB Office of the Federal Chief Information Officer FY *2022 Core IG Metrics Implementation Analysis and Guidelines*.
- Council of the Inspectors General on Integrity and Efficiency (CIGIE), OMB, DHS, and the and the Federal Chief Information Officers and Chief Information Security Officers councils *FY 2022 Core IG FISMA Metrics Evaluation Guide.*
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* for specification of security controls.
- NIST SP 800-37, Revision 2, *Guide for Applying the Risk Management Framework to Federal Information Systems,* for the risk management framework controls.
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* for specification of security controls.
- NIST SP 800-53A*,* Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations,* for the assessment of security control effectiveness.
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment.*
- NIST SP 800-161, Revision 1, Cybersecurity *Supply Chain Risk Management Practices for Systems and Organizations.*
- OMB A-130, July 28, 2016, *Managing Information as a Strategic Resource.*
- Public Law 115-390 -115th Congress, *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the "Secure Technology Act."*

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 the fiscal year 2022. Based on these efforts we determined that nine prior-year recommendations were closed, and 42 recommendations were determined still open as of September 9, 2022.

Prior Years' FISMA Recommendations that Were Closed

Fiscal Year 2015, OIG Report Number 16-02 Audit of NARA's Compliance with FISMA	
Number	**Recommendation**
4	The CIO should develop, update, and implement formalized access control policies and procedures for four systems.

Fiscal Year 2018, OIG Report Number 19-AUD-02 Audit of NARA's Compliance with FISMA	
Number	**Recommendation**
2	Ensure SSPs are developed for all NARA systems in accordance with NARA policy.
3	Ensure SSPs are reviewed and updated for all NARA systems in accordance with NARA policy to ensure any missing control implementation details are completed, and missing privacy controls added.
9	Assign ISSO's for all major applications and general support systems.
17	Ensure user access request forms are retained for each user account on all systems.
18	Ensure individuals assigned elevated privileges have their user accounts disabled if they have not completed their security awareness training by their scheduled completion date.
27	Test the contingency plans for all NARA systems to include documentation of test plans, results and any needed updates to the contingency plan, and establish controls to ensure annual testing of contingency plans.

Fiscal Year 2021, OIG Report Number 22-AUD-04 Audit of NARA's Compliance with FISMA	
Number	**Recommendation**
8	Identify all system security plans, which are missing attributes, then update so these values are populated.
9	Conduct a security control assessment of one system, with results documented within a Security Assessment Report (SAR).

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 2015, OIG Report Number 16-02 Audit of NARA's Compliance with FISMA	
Number	**Recommendation**
1	The CIO should 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.
13	For future agreements, the CIO should: • 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.
14	The CIO should add an addendum to current agreements which requires compliance with NARA's information security requirements.
20	The CIO should implement the following corrective actions: • Complete efforts to implement the Security Information and Event Management product, • Develop and implement processes and procedures to monitor and at least weekly review user activity and audit logs (in accordance with NARA IT Security Requirements), on five 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.

Fiscal Year 2018, OIG Report Number 19-AUD-02 Audit of NARA's Compliance with FISMA	
Number	**Recommendation**
1	Ensure complete security authorization packages for each major application and general support system are completed prior to deployment into production.
4	Conduct risk assessments for each system in operation and establish policies or procedures to ensure that risk assessments are conducted at least annually.
6	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 the corrective actions.
8	Ensure IT policies, procedures, methodologies, and supplements are reviewed and approved in accordance with NARA Directive 111.
12	Implement improved processes to remediate security deficiencies on NARA's network infrastructure, to include enhancing its patch and vulnerability

Fiscal Year 2018, OIG Report Number 19-AUD-02 *Audit of NARA's Compliance with FISMA*	
Number	**Recommendation**
	management program to address security deficiencies identified during our assessments of NARA's applications and network infrastructure.
13	Ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported.
15	Ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy.
16	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."
20	Ensure audit logging is enabled for each major information system.
21	Ensure periodic reviews of generated audit logs are performed for each major information system.
22	Ensure password configuration settings for all major information systems are in accordance with NARA IT Security Requirements.
23	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.
24	Ensure a process is developed, documented, and implemented to change passwords whenever users within shared/group accounts change.

Fiscal Year 2021, OIG Report Number 22-AUD-04 *Audit of NARA's Compliance with FISMA*	
Number	**Recommendation**
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.
4	Ensure inconsistencies described regarding the POA&M closure process stated within and between the CFM, NARA IT Security Methodology for Certification and Accreditation (CA) and Security Assessments, and the NARA ISSO Guide are identified and resolved.
5	Identify all FISMA reportable systems in which the AO listed within the ATO, has subsequently changed.
6	For those systems identified in which the AO listed in the ATO has changed, NARA should 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.
7	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.

Fiscal Year 2021, OIG Report Number 22-AUD-04 *Audit of NARA's Compliance with FISMA*	
Number	**Recommendation**
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.
11	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.
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.
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.
21	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
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.
23	Develop and implement a configuration management plan for one system in accordance with NARA's configuration management plan templates, policies, and procedures.
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.

Fiscal Year 2021, OIG Report Number 22-AUD-04 *Audit of NARA's Compliance with FISMA*	
Number	**Recommendation**
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 network 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.
33	The Senior Agency Official for Privacy (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.
35	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, so commensurate with the availability risk level assigned.

Appendix D: Acronyms

AO	Authorizing Official
ATO	Authorization to Operate
BIA	Business Impact Analysis
CA	Certification and Accreditation
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CFM	Cybersecurity Framework Methodology
CIO	Chief Information Officer
CLA	CliftonLarsonAllen LLP
CM	Configuration Management
COVID	Coronavirus Disease
DHS	Agency 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	Inspector General
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
IT	Information Technology
MFA	Multifactor Authentication
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OST	Office of the Secretary
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plans of Actions and Milestones
RMF	Risk Management Framework
RTO	Recovery Time Objective
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SAT	Security Awareness Training

SCA	Security Control Assessment
SCRM	Supply Chain Risk Management
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plans
TT&E	Test, Training and Evaluation
US-CERT	United States Computer Emergency Readiness Team

Appendix E: Agency Comments

Agency management reviewed the discussion draft and provided comments that have been incorporated in this report, as appropriate. 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

Acting 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

Government Accountability Office

United States House Committee on Oversight and Government Reform

Senate Homeland Security and Government Affairs Committee

OIG Hotline

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 the Hotline email system and 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 email
oig.hotline@nara.gov

By facsimile
301-837-3197

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

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 *www.archives.gov/oig/contractor-form/index.html*.